MASTER'S THESIS

Implementatie van Continuous Compliance

Automatisering van Information Security Measures binnen het softwareontwikkelproces om Continuous Compliance te bewerkstelligen

Ozkanli, N (Nese)

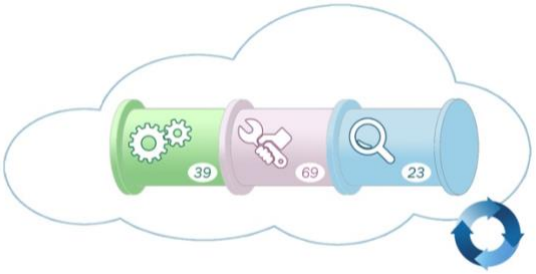
Award date:
2020

Implementatie van Continuous Compliance

Automatisering van Information Security Measures binnen het softwareontwikkelproces om Continuous Compliance te bewerkstelligen

Implementation of Continuous Compliance

Automation of Information Security Measures in the software development process to ensure Continuous Compliance



Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeertraject Business Process Management and IT
Student:	Nese Ozkanli
Identiteitsnummer:	
Datum:	10 juni 2020
Afstudeerbegeleider	Prof. dr. Yuri Bobbert
Meelezer	dr. Anda Counotte-Potman
Derde beoordelaar	Prof. dr. Rob Kusters
Versie nummer:	1.7
Status:	Definitief

Voorwoord

Voor Nese Ozkanli

Het is een grote eer als je een voorwoord mag schrijven. Als dit ook nog eens een voorwoord is voor iemand die besluit om naast werk en privé veel tijd en energie te steken in een universitaire opleiding dan kan ik daar alleen maar veel respect voor hebben. Mijn complimenten voor jou om deze stap te zetten en te realiseren en dat op een onderwerp die gerust 'hot' mag worden genoemd. Ik heb je scriptie mogen lezen en ik wil je van harte aanraden om hier een paper/artikel van te maken.

Op naar Continuous Integration / Continuous Delivery

Door de komst van agile, scrum en DevOps zijn compliance vraagstukken als functiescheiding weer terug. Jarenlang kon de IT-auditor roepen dat een Ontwikkelaar (Developer) niet op de productie omgeving mocht komen (Operations) vanwege functiescheiding. Immers een ontwikkelaar op de productie omgeving is in staat om frauduleuze code te onderhouden. Echter echte agility betekent dat een DevOps team kan leven bij het principe: je bouwt het, je beheert het en je repareert het. Bestaande compliance raamwerken hebben moeite met deze ontwikkeling. Immers dan is die frauduleuze ontwikkelaar weer in staat om de boel te bedonderen, en dat is niet de bedoeling.

Op naar Continuous compliance

Ik ben ervan overtuigd dat het weldegelijk mogelijk is om echte DevOps te realiseren maar wil dat graag benoemen als DevSecOps (Sec is Security). Hiervoor zijn echter vernieuwde compliance controls nodig en Nese heeft hier een mooie aanzet voor gegeven. In mijn praktijk als CISO gebruik ik zelf een aantal hoofd vereisten om DevSecOps mogelijk te maken en Nese refereert al aan het A-SAMM model welke de basis is. Daarnaast gebruik ik als major controls: (1) Fully automated CI/CD pipeline, wat inhoudt dat alle stappen geautomatiseerd zijn / te volgen zijn. (2) 4 ogen principe (de een bouwt en de ander controleert (binnen een team). (3) extensive logging (alle stappen worden gelogd zodat er een audit(trail) is op de gebouwde, beheerde en gerepareerde code) en (4) breakthrough infrastructuur access glass wat betekent dat er een alarm afgaat als een DevSecOps team op de infra komt en uiteraard moet dat ook allemaal gelogd worden.

Bovenstaande in combinatie met het mooie overzicht van Nese vormt een goede basis voor het verder ontwikkelen van een Continuous Compliance Framework.

Voor mij in de rol van CISO zie ik duidelijk de behoefte aan de verdere ontwikkeling van een dergelijk raamwerk. Nese, dank voor jouw bijdrage hieraan, een stap voor een groeiend en gewenst vakgebied.

Beste lezer, heel veel leesplezier en laat u leiden in de gedachten en bevindingen.

Prof. dr. Barry Derksen

Professor aan Antwerp Management School

Bestuurslid Secure Software Alliance & ISACA NL chapter

Auteur van het boek Agile Secure Software Lifecycle Management

Abstract

Organisaties kiezen steeds vaker om kort cyclisch software te ontwikkelen en te implementeren met Agile methoden. Een gevolg van deze kort cyclische softwareontwikkelmethoden is dat ook rekening gehouden moet worden met compliance wat in traditionele methoden meestal veel handmatig werk vergt. Door Information Security Measures vroegtijdig en geautomatiseerd in het ontwikkelproces mee te nemen kan op een beheerste manier software snel geïmplementeerd worden.

De doelstelling van dit onderzoek is het bepalen van welke Information Security Measures geautomatiseerd kunnen worden in Continuous Deployment Pipelines zodat een Continuous Compliance framework bewerkstelligd kan worden.

Uit een uitgebreid literatuuronderzoek is gebleken dat er geen éénduidige manier en/of overzicht is om Information Security Measures geautomatiseerd te integreren in Continuous Deployment Pipelines. Tijdens het empirisch onderzoek is met zes experts onderzocht welke Information Security Measures, die gebaseerd zijn op het Information Security Forum framework Standard of Good Practice (2018), geautomatiseerd kunnen worden in Deployment Pipelines. Het resultaat van dit onderzoek is een Continuous Compliance Framework dat een uitgebreid overzicht geeft van Information Security Measures die variërend van eenvoudig tot moeilijk geautomatiseerd kunnen worden binnen Deployment Pipelines. Deze lijst kan binnen organisaties gebruikt worden om roadmaps te prioriteren en de volgorde van implementaties te bepalen.

Sleutelbegrippen

Design Science Research, Regulatory Technology, Continuous Compliance Framework, Continuous Delivery, Continuous Deployment Pipeline, Information Security Measures, Security Controls, Security Automatisering, Security Automation, Risk management.

Samenvatting

Vandaag de dag willen veel bedrijven door diverse redenen steeds sneller software implementeren om de time-to-market periode te verkorten. Om deze reden wordt steeds vaker gekozen om kort cyclisch software te ontwikkelen en te implementeren met Agile methoden. Een gevolg van deze kort cyclische softwareontwikkelmethoden is dat ook rekening gehouden moet worden met compliance wat in traditionele methoden veel handmatig werk vergt. Door Information Security Measures vroegtijdig en geautomatiseerd in het ontwikkelproces mee te nemen kan men op een beheerste manier software snel implementeren. Deze kort cyclische ontwikkelmethode gebeuren vaak met software straten waarin meerdere personen werken aan de 'lopende band' om software tot een goed eindproduct te brengen. We spreken dan over de Engelse term Deployment Pipelines (Ontwikkelstraat).

De doelstelling van dit onderzoek is het bepalen van welke Information Security Measures geautomatiseerd kunnen worden in Continuous Deployment Pipelines zodat een Continuous Compliance framework bewerkstelligd kan worden wat bruikbaar is voor de praktijk.

Uit een uitgebreid literatuuronderzoek is gebleken dat er geen éénduidige manier is om Information Security Measures geautomatiseerd te integreren in een Continuous Deployment Pipeline. Tevens is er geen duidelijk definitie te vinden in de huidige literatuur. Om die reden is tijdens het empirisch onderzoek een definitie gedestilleerd aan de hand van de antwoorden van de experts voor Continuous Compliance:

Middels door interne en/of externe regelgeving vooraf gedefinieerde Information Security en Privacy policies en standaarden de nodige maatregelen (measures) inrichten binnen deployment pipelines om de daarbij behorende doelstellingen via controlemaatregelen effectief en continu te realiseren, te administreren en over te rapporteren naar relevante stakeholders.

De resultaten van het literatuuronderzoek hebben aangetoond dat het Information Security Forum (ISF) Standard of Good Practice (2018) het meest uitgebreide security framework is. Dit omdat ISF de meeste security frameworks die in de literatuur zijn genoemd afdekt. Om deze reden is het ISF framework als vertrekpunt genomen om het empirisch onderzoek vorm te geven.

Tijdens het empirisch onderzoek is met experts onderzocht welke Information Security Measures, die gebaseerd zijn op het ISF framework, geautomatiseerd kunnen worden in Deployment Pipelines. Het resultaat van dit onderzoek is een Continuous Compliance Framework dat een uitgebreid overzicht geeft van Information Security Measures die variërend van eenvoudig tot moeilijk geautomatiseerd kunnen worden binnen een Deployment Pipeline. Deze lijst kan uitermate goed van toepassing komen binnen organisaties om software ontwikkel strategieën en roadmaps te prioriteren en betere volgordelijkheid aan implementaties te geven.

Aan de hand van de uitkomsten van dit onderzoek kunnen organisaties in veel hogere mate bepalen of ze de juiste dingen doen en of ze die dingen ook echt goed doen. Met name als het gaat om security en compliance eisen ten aanzien van softwareontwikkeling. Aan dit onderzoek werkten mee zes experten binnen één financiële instelling.

Summary

Today, many companies want to implement software faster to shorten the time-to-market period for various reasons. Because of this, the choice is made increasingly to develop and implement short-cycle software with Agile methods. A consequence of these short-cycle software development methods is that compliance must also be considered, which requires a lot of manual work in traditional methods. By including Information Security Measures early and automated in the development process, software can be implemented quickly in a controlled manner. This short-cycle development method often happens with software streets in which several people work on the 'assembly belt' to bring software to a good end product.

The aim of this research is to determine which Information Security Measures can be automated in Continuous Deployment Pipelines so that a Continuous Compliance framework can be achieved.

An extensive literature search has shown that there is no unambiguous way and / or overview to automatically integrate Information Security Measures into a Continuous Deployment Pipeline. There is also no clear definition of Continuous Compliance in the current literature. For this reason, a definition was distilled during the empirical study based on the answers of the experts for Continuous Compliance:

Establish the necessary measures within deployment pipelines through Information Security and Privacy policies and standards that are predefined by internal and / or external regulations to achieve and administer the associated objectives effectively and continuously via control measures and to report these to relevant stakeholders.

The results of the literature search have shown that the Information Security Forum (ISF) Standard of Good Practice (2018) is the most comprehensive security framework. This is because ISF covers most of the security frameworks which are mentioned in the literature. For this reason, the ISF framework has been taken as the starting point to shape the empirical research.

During the empirical study, experts examined which Information Security Measures, which are based on the ISF framework, can be automated in Deployment Pipelines. The result of this research is a Continuous Compliance Framework that provides a comprehensive overview of Information Security Measures that can be automated from simple to difficult within a Deployment Pipeline. This list can be extremely useful within organizations to prioritize software development strategies and roadmaps and to give better order sequences to implementations.

Based on the results of this research, organizations can determine to a much greater extent whether they are doing the right things and whether they are actually doing those things well. Especially when it comes to security and compliance requirements with regard to software development. Six experts within one financial institution participated in this study.

Inhoudsopgave

Voorwoord ii
Abstract iii
Sleutelbegrippen iii
Samenvatting iv
Summary v
Inhoudsopgave vi
1. Introductie 1
1.1. Inleiding 1
1.2. Gebiedsverkenning 3
1.3. Aanleiding / relevantie 5
1.4. Probleemstelling 5
1.5. Opdrachtformulering 7
1.6. Aanpak in hoofdlijnen 8
2. Theoretisch kader 9
2.1. Onderzoeksaanpak 9
2.1.1. Doel literatuuronderzoek 9
2.1.2. Aanpak literatuuronderzoek 9
2.1.3. Zoektermen 11
2.1.4. Zoekbronnen 12
2.1.5. Selectieproces 12
2.2. Uitvoering literatuuronderzoek 13
2.2.1. Continuous Compliance Framework 13
2.2.2. Information Security Frameworks in Deployment Pipelines 15
2.2.3. Information Security Measures in Deployment Pipelines 16
2.2.4. Automatisering van Information Security Measures 18
2.3. Resultaten en conclusies 20
2.3.1. Continuous Compliance Framework 20
2.3.2. Information Security Frameworks in Deployment Pipelines 21
2.3.3. Information Security Measures in Deployment Pipelines 23
2.3.4. Automatisering van Information Security Measures 25
2.3.5. Conclusie literatuuronderzoek 27
2.4. Doel van het vervolgonderzoek 28
3. Methodologie 29

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n) 29
3.1.1. Deductief of Inductief? 29
3.1.2. Kwalitatief of kwantitatief? 29
3.1.3. Welke onderzoeksmethoden? 29
3.1.4. Ontwerpgericht onderzoek 30
3.2. Technisch ontwerp: uitwerking van de methode 32
3.3. Gegevensanalyse 36
3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten 36
4. Resultaten 39
4.1. Uitvoering onderzoek 39
4.2. Continuous Compliance Framework 40
4.3. Information Security Frameworks 40
4.4. Information Security Measures in Continuous Deployment Pipelines 41
4.5. Automatisering van Information Security Measures 41
5. Conclusie, discussie en aanbevelingen, reflectie 45
5.1. Discussie 45
5.2. Conclusie 47
5.3. Aanbevelingen voor de praktijk 48
5.4. Aanbevelingen voor verder onderzoek 49
5.5. Reflectie 49
Referenties 51
Figurenlijst 53
Tabellenlijst 53
Bijlage 1 - Zoekresultaten literatuuronderzoek 54
Bijlage 1.1 - Zoekresultaten deelvraag 1 55
Bijlage 1.2 - Zoekresultaten deelvraag 2 58
Bijlage 1.3 - Zoekresultaten deelvraag 3 63
Bijlage 1.4 - Zoekresultaten deelvraag 4 67
Bijlage 2 - Voorbereiding participant op het interview 69
Bijlage 3 - Interview protocol 71
Bijlage 4 - Automatable Information Security Measures 73
Bijlage 5 - Transcripten interviews 85
Bijlage 6 - Framework voor Continuous Compliance 85

1. Introductie

1.1. Inleiding

De financiële sector is een snel veranderende omgeving, bedrijven in deze sector moeten om hun bestaansrecht te kunnen behouden steeds sneller reageren op de vragen van de markt, de wensen en behoeften van de klanten en eventuele wettelijke wijzigingen. Volgens Oppenheim, Stenson & Wilson (2003) is in snel veranderende en concurrerende zakelijke omgevingen flexibiliteit van cruciaal belang en spelen informatiebronnen en hun kenmerken een rol. Daarnaast geven Oppenheim et al. (2003) aan dat klanten en producten met succes verbonden moeten worden om aan de eisen van snel veranderende markten te kunnen voldoen, dit omdat klanten steeds veeleisender worden Forsgren, Humble, and Kim (2018); (Oppenheim, Stenson, & Wilson, 2003).

De digitalisering en automatisering van de bedrijfsprocessen vereist eveneens dat bedrijven snel reageren om klanten tevreden te houden.
Weill & Woerner (2015) stellen dat het bedrijfsleven snel digitaliseert en dat dit nieuwe kansen met zich meebrengt terwijl de bedrijfsmodellen die lang als succesvol werden gezien hiermee vernietigd worden. Om voor de toekomst voorbereid te zijn, geven ze aan dat bedrijven mogelijkheden moeten creëren en competenties moeten ontwikkelen op twee gebieden. In het eerste gebied wordt benoemd dat bedrijven hun klanten beter moeten leren kennen en in het tweede gebied wordt gesteld dat bedrijven meer een onderdeel moeten zijn van een ecosysteem. Om een onderdeel te worden van een ecosysteem geven ze onder andere aan dat het nodig is om efficiëntie en compliance als een competentie te behandelen.
Tevens geven Weill & Woerner (2015) aan dat succes ook een verhoogde digitalisering van de activiteiten binnen een bedrijf vereist, waarbij de inherente potentiële efficiëntie, verantwoordelijkheden en bedreigingen worden herkend. Deze omvatten het omgaan met dataprivacykwesties, cyberbedreigingen, mogelijke verstoring van de dienstverlening en de noodzaak van toenemende mate van toezicht op naleving door overheden en andere toezichthouders wereldwijd. Bedrijven die dit allemaal kunnen doen, maken compliance een competentie en zullen ernaar streven de beste in hun klasse te zijn (Weill & Woerner, 2015).

Tegenwoordig wordt software ontwikkeld in snel veranderende en onvoorspelbare markten waarbij complexe en steeds veranderende eisen van klanten druk leggen om de time-to-market periode te verkorten. Agile methoden hebben de mogelijkheden voor bedrijven die software ontwikkelen vergroot om aan complexe en veranderende eisen van klanten en aan veranderende marktbehoeften te voldoen (Claps, Svensson, & Aurum, 2014).

Om deze redenen is de Agile softwareontwikkelmethode genaamd Continuous Delivery tegenwoordig een onderwerp met veel aandacht dat veel van deze doelen ondersteunt. Continuous Delivery is een moderne softwareontwikkelmethode waarmee nieuwe functionaliteit snel en efficiënt geïmplementeerd kan worden. Chen (2015) definieert Continuous Delivery als een aanpak voor softwareontwikkeling waarin ontwikkelteams kortcyclisch waardevolle software produceren en ervoor zorgen dat de software op een betrouwbare manier op elk moment geïmplementeerd kan worden (L. Chen, 2015). Een gevolg van deze kort cyclische softwarereleasemethode is dat ook beveiligingseisen vroegtijdig in het ontwikkelproces moeten worden meegenomen. Indien dit onvoldoende gebeurt loopt men de kans dat er foutieve software met 'gaten' wordt vrijgegeven. Dit wordt nog complexer als meerdere bouwers aan dezelfde code werken tijdens een Continuous Delivery proces (Visser, Rigal, van der Leek, van Eck, & Wijnholds, 2016).

Om de voordelen van Continuous Delivery te kunnen behalen, is het van belang dat instellingen enerzijds veilige code ontwikkelen en anderzijds ook rekening houden met het opleveren van relevant bewijsmateriaal tijdens het doorvoeren van softwarewijzigingen. Dit is nodig voor de administratieve organisatie, interne controle en voor toezichthouders. Deze “checks and balances” dienen te worden ingebouwd zonder de snelheid van Continuous Delivery in gevaar te brengen.

Financiële instellingen zijn volgens "De Nederlandse grondwet" (2019), het Europees parlement en de raad van de Europese Unie onderhevig aan macroprudentieel toezicht. Macroprudentieel toezicht richt zich op de soliditeit van het financiële stelsel als geheel.
De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), de Autoriteit Persoonsgegevens (AP) en het Nationaal Cyber Security Centrum (NCSC) zijn verantwoordelijk voor het uitvoeren van dit toezicht. Door regels en richtlijnen die hieruit voortvloeien zijn financiële instellingen belast met het opleveren van voldoende bewijsmateriaal bij onder andere het doorvoeren van veranderingen in hun systemen of proces. Daarnaast worden ook regelmatig interne en externe audits uitgevoerd waarbij veel bewijsmateriaal geleverd moet worden om de effectiviteit van de controls aan te tonen.

Naast het externe toezicht zijn er ook bedrijfsrichtlijnen die vanuit de administratieve organisatie gesteld worden. Door middel van interne controle wordt binnen veel bedrijven ook toezicht gehouden of de richtlijnen goed toegepast worden en getoetst of controle maatregelen daadwerkelijk effectief zijn.
Volgens de website van "The Institute of International Auditors," (2019) is het management verantwoordelijk voor het bepalen van beleid, het monitoren van de prestaties en het nemen van corrigerende maatregelen als het beleid of de uitvoering ervan gebrekkig is. Het instituut geeft aan dat interne controlesystemen van fundamenteel belang zijn voor het succes en het voortbestaan van organisaties. Ze houden de organisatie op de rails. Interne controle wordt door het instituut gedefinieerd als een proces binnen een organisatie dat is ontworpen om redelijke zekerheid te bieden met betrekking tot de volgende primaire bedrijfsdoelstellingen:

- Betrouwbaarheid en integriteit van informatie
- Naleving van beleid, plannen, procedures, wetten en voorschriften
- Het beschermen van de activa
- Het economische en efficiënte gebruik van resources
- De verwezenlijking van vastgestelde doelstellingen en doelstellingen van operaties of programma's

In Nederland worden deze richtlijnen, de bijbehorende educatie en praktijken door het NOREA vormgegeven. Zeni, Kiyavitskaya, Mich, Cordy, & Mylopoulos (2013) geven in hun onderzoek aan dat verschillend internationaal beleid, wetten en voorschriften, geschreven in een breed scala van talen, zelfs binnen één rechtsgebied, zoals de Europese Unie, samen met privacy en beveiligingsvereisten wereldwijd een serieuze uitdaging voor softwareontwikkelaars vormt. In het bijzonder moeten IT-professionals het hoofd bieden aan het zogenaamde compliance-probleem, waarbij bedrijven en ontwikkelaars wordt gevraagd om ervoor te zorgen dat hun softwaresystemen voldoen aan de relevante voorschriften, hetzij door ontwerp of door re-engineering (Zeni et al., 2013).

Het doel van dit afstudeeronderzoek is om te onderzoeken hoe de richtlijnen die vanuit de interne organisatie en toezichthouders voortvloeien in het softwareontwikkelproces ondersteund en geautomatiseerd kunnen worden.

Leeswijzer

Dit document bestaat uit vijf onderdelen. Hoofdstuk één is de inleiding waarin de probleemstelling, relevantie en opdrachtformulering wordt beschreven. In Hoofdstuk twee wordt de literatuurstudie behandeld. Op basis van de uitkomsten uit de literatuurstudie wordt het empirisch onderzoek opgezet in Hoofdstuk drie. In Hoofdstuk vier worden de resultaten van het empirisch onderzoek behandeld en tot slot wordt in Hoofdstuk vijf de conclusie en aanbeveling gegeven dat afgesloten wordt met een reflectie op het onderzoeksproces.

1.2. Gebiedsverkenning

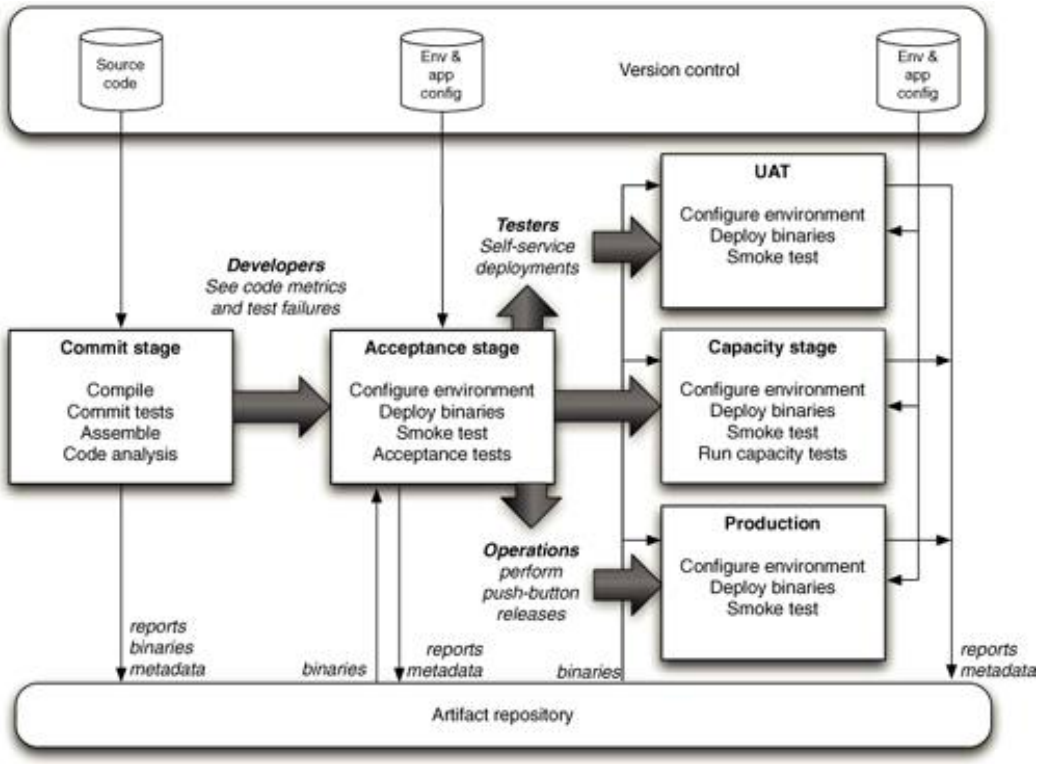
Humble & Farley (2010) stellen dat Continuous Delivery meer is dan alleen een nieuwe methode om software te leveren. Het is een geheel nieuwe paradigma voor het runnen van een bedrijf dat afhankelijk is van software. Het implementeren van Continuous Delivery vergt volgens hen meer dan alleen het aanschaffen van een aantal tools en de automatisering van handmatig werk. Het hangt af van effectieve samenwerking tussen alle betrokkenen in de levering van de software, ondersteuning van executive sponsors en de bereidheid van de mensen op de werkvloer om wijzigingen aan te brengen.

De focus van organisaties ligt veelal bij de keuze van de juiste tooling die nodig is om automatisch software te kunnen testen of automatisch te kunnen uitrollen (nader te adresseren als 'deployen'). Humble & Farley (2010) stellen ook dat de beginfase (inception) van een project erg belangrijk is. Het kan erg verleidelijk zijn om deze fase over te slaan, maar zelfs de "hardcore agilista authors" hebben uit bittere ervaring geleerd dat deze fase zorgvuldig gepland en uitgevoerd dient te worden om een softwareproject succesvol te laten zijn. Een deliverable uit deze beginfase is bijvoorbeeld een lijst van high-level functional en non-functional requirements met precies genoeg detail om het werk in te kunnen schatten en het project te plannen (Humble & Farley, 2010).

Lu, Lin, Huang, & Yuan (2017) geven in hun onderzoek aan dat Johnson (2015) van de Standishgroup gerapporteerd heeft dat op meer dan 50.000 softwareprojecten in de Verenigde Staten 31,1% van de projecten wordt geannuleerd voordat ze ooit worden voltooid. 52,7% daarvan kost 189% meer dan hun oorspronkelijke begrotingen, er zijn slechts 16,2% van de softwareprojecten die op tijd en binnen het budget zijn voltooid, en het aantal wordt verlaagd tot 9% voor grotere bedrijven. Zelfs bij voltooide projecten wordt slechts ongeveer 42% van de oorspronkelijk voorgestelde functionaliteit en functies geïmplementeerd. Met zulke onthutsende cijfers is het duidelijk dat er iets mis moet zijn in het softwareontwikkelingsproces. De twee belangrijkste factoren die ervoor zorgden dat een softwareproject faalde of werd aangevochten, waren onvolledige requirements en een gebrek aan gebruikersbetrokkenheid (Lu et al., 2017).

Om de vereiste beveiligingsmaatregelen, onder andere in de softwarecode goed te implementeren en te onderhouden dienen deze maatregelen en requirements ook afgestemd te worden op Continuous Delivery implementaties. Men kan denken aan allerlei soorten van checks en balances zoals toegangscontrole tot de code, logging en monitoring, versleuteling en of tussentijds testen op

“lekken” in de softwarecode. Om maximale efficiëntie in het afwerken van deze checks en balances in het Continuous Delivery softwareontwikkelproces te houden is het noodzakelijk om zoveel mogelijk bewijslast dat voortvloeit uit het ontwikkelproces te automatiseren. Humble & Farley (2010) geven aan dat er een aantal voorschriften automatisch afgedwongen kunnen worden in een Deployment Pipeline. Ze leggen uit dat een Deployment Pipeline een geautomatiseerd proces is om software via een version control systeem beschikbaar te maken aan gebruikers. In dit geautomatiseerd proces wordt de software ontwikkeld, in meerdere fases getest en geïmplementeerd op productie. Figuur 1 toont welke fases de broncode moet doorlopen om op een veilige en gecontroleerde manier software te implementeren op productie.



Figuur 1: Basic Deployment Pipeline (Humble & Farley, 2010)

Binnen de Deployment Pipeline is het bijvoorbeeld mogelijk om vast te leggen wie bij de beveiligde omgevingen mogen komen, wie, wanneer, welke wijziging heeft aangebracht in de software, welke testen geslaagd en welke testen gefaald zijn etc.. Dit wordt door practitioners ook wel Continuous Compliance genoemd.

Long (2015) definieert Continuous Compliance als volgt "Een continu proces van proactief risicobeheer dat voorspelbare, transparante en kosteneffectieve resultaten oplevert om aan de doelstellingen van informatiebeveiliging te voldoen." Fischl Bodner (2018) definieert Continuous Compliance als het bereiken van een staat waarin aan alle nalevingsvereisten is voldaan, en vervolgens het continu onderhouden van die staat. Een andere definitie is van Prins (2016) en dat luidt als: "Continuous Compliance is de uitkomst van de inrichting van het voortbrengingsproces van software waarbij elke stap geautomatiseerd bewijslast oplevert en ook zelf zo is ingericht dat onomstotelijk kan worden vastgelegd hoe een change is uitgevoerd."

1.3. Aanleiding / relevantie

Vandaag de dag is op het gebied van Continuous Delivery en Deployment Pipelines het een en ander onderzocht, maar is het aantal onderzoeken naar de automatisering van Continuous Compliance binnen de Deployment Pipelines beperkt. Dit omdat Continuous Compliance een vrij nieuw paradigma is waar nog weinig wetenschappelijk onderzoek naar is gedaan. Door onder andere snel veranderende regels en richtlijnen is het van belang voor bedrijven die onderhevig zijn aan intern en extern toezicht dat het compliance proces goed is ingericht en zoveel mogelijk geautomatiseerd. Hiermee kan voorkomen worden dat bijvoorbeeld softwareontwikkelaars, IT-Professionals, veel tijd en geld besteden aan het verzamelen van alle bewijsmateriaal dat nodig is voor zowel interne audits als externe toezichthouders. Deze toezichthouders hebben dit op hun beurt nodig om een bepaalde mate van “reasonable assurance”, oftewel zekerheid van integriteit van informatie te kunnen vaststellen.
De resultaten van dit onderzoek zullen een bijdrage leveren aan de wetenschappelijk kennis omtrent Continuous Compliance methoden.

Daarnaast zal dit onderzoek een bijdrage leveren aan bedrijven die Compliance willen automatiseren binnen hun eigen Continuous Delivery software ontwikkelproces.

1.4. Probleemstelling

Om kritische en niet kritische bedrijfsapplicaties van elkaar te onderscheiden, wordt er vaak binnen bedrijven een Business Impact Analysis (BIA) uitgevoerd. Sikdar (2011) geeft in zijn onderzoek aan dat de BIA een hulpmiddel is om processen die moeten worden voortgezet, hun prioriteit en de middelen die nodig zijn om deze processen uit te voeren, te identificeren.

Op basis van onder andere de data die verwerkt wordt in de applicatie, wordt tijdens het BIA-proces een classificatie vastgesteld waarmee vervolgens bepaald kan worden welke beveiligingsmaatregelen, nader te noemen als security measures, binnen een bepaalde omgeving toegepast moeten worden. Deze measures worden vandaag de dag veelal handmatig gedocumenteerd en meestal bijgehouden in spreadsheets. Bij het handmatig bijhouden van registratie van security measures bestaat een verhoogd risico op fouten. Handmatige handelingen zijn niet goed schaalbaar, moeilijker controleerbaar en de controle is vaak gebaseerd op momentopnames of op basis van selecties van momentopnames. Door deze momentopnames ontstaan problemen omdat de gedocumenteerde gegevens snel verouderen. Hierdoor wordt versiebeheer van documentatie een lastig bij te houden fenomeen.
Bobbert & Mulder (2019) geven in hun onderzoek aan dat het invullen van spreadsheets met antwoorden op questionnaires onderworpen is aan manipulatie omdat het geen gesloten lus is. Spreadsheet data is gelimiteerd tot subjectieve meningen en er is weinig ruimte voor reflectie. Daarnaast kan spreadsheet data niet altijd verzameld worden via originele bronnen waardoor de authenticiteit en integriteit wordt vermindert (Bobbert & Mulder, 2019).

Powell, Baker, & Lawson (2009) hebben in hun onderzoek naar de impact van fouten in operationele spreadsheets aangetoond dat fouten in spreadsheets in meer varianten kunnen voorkomen. Omdat het spreadsheetplatform zo ongestructureerd is en omdat eindgebruikers over het algemeen unieke ontwerpen volgen, kunnen fouten in duizenden verschillende varianten manifesteren.

Zitting (2015) geeft aan dat naast het feit dat spreadsheets een slechte plek zijn om samen te werken, er ook aanzienlijke risico's verbonden zijn aan het gebruik van gedeelde spreadsheets. Het is bijvoorbeeld erg makkelijk om een formulefout te maken en het kan lastig zijn om een audittrail van het werk bij te houden. Het is ook niet goed mogelijk om de toegang tot gegevens in een spreadsheet te beheren. Tevens kunnen bestanden beschadigd raken of verloren gaan in de chaos van versiebeheer (Zitting, 2015).

Bobbert (2017) concludeert in zijn case study in *Security, Risk and Compliance artefact engineering* dat het verzamelen van gegevens van meerdere security tooling (bijvoorbeeld firewalls), gecombineerd met checklists die bewijs vereisen, zoals bij audits, virtualisatie en cloud-audits, niet haalbaar is met spreadsheets (Bobbert, 2017).

Humble & Farley (2010) stellen dat veel bedrijven beweren dat handmatige documentatie centraal staat bij auditen en geven aan dat deze denkwijze moet veranderen. Een document geeft aan dat iets is uitgevoerd op een bepaalde manier en dat dit niet bewijst dat het ook daadwerkelijk is uitgevoerd. Documentatie heeft de nare gewoonte om te verouderen. Hoe gedetailleerder het document, hoe sneller het veroudert (Humble & Farley, 2010).

Security controls die onder andere voortvloeien vanuit bepaalde regelgeving, richtlijnen, architectuur en de business zijn meestal complexe begrippen waar specifieke en diepgaande technische kennis voor nodig is. Daarnaast is het meestal ook onduidelijk beschreven welke specifieke security controls geïmplementeerd moeten worden en worden deze controls ook in complexe spreadsheets beheerd. Om deze redenen vinden IT-medewerkers het in de beginfase vaak lastig om deze security controls te vertalen in concrete handelingen.

Het softwareontwikkelproces wordt meer en meer geautomatiseerd en gaat met de huidige technieken die op de markt beschikbaar zijn steeds sneller en het wordt steeds meer geïntegreerd met security en compliance controls. Indien organisaties op de oude manier, namelijk handmatig, in spreadsheets blijven werken om hun complianceproces en security controls te beheren en dit handmatig overtypen, zal dit op een gegeven moment een knelpunt gaan vormen en o.a. het Continuous Delivery proces gaan vertragen.

Het handmatig verzamelen van bewijsmateriaal is een probleem dat bijna alle dimensies van een organisatie raakt. Van de business die de time-to-market wil verkorten om hun klanten sneller te kunnen bedienen tot aan de softwareontwikkelaar die niet kan focussen op zijn eigen werk doordat er steeds handmatig bewijslast geleverd moet worden. Denk hierbij ook aan het Management dat geen overzicht heeft over de totale organisatie omdat alle documentatie verspreid is over meerdere locaties in verschillende spreadsheets.

Het probleem is dat spreadsheet management een risico op zich begint te worden naarmate de organisatie groter wordt, regelgeving hogere kwaliteit en actualiteitseisen stelt, software changes sneller plaats moeten vinden en handmatige documentatie deze snelheid niet meer kan bijbenen.

De centrale probleemstelling in deze thesis is daarom als volgt geformuleerd: **Doordat veel bedrijven Information Security Measures op een handmatige manier in spreadsheets bijhouden zullen zij vertraagd worden in het softwareontwikkelproces en niet de voordelen zoals snelheid en veiligheid van Continuous Delivery behalen.**

1.5. Opdrachtformulering

Om de snelheid van Continuous Delivery te behalen is het hoognodig om zoveel mogelijk de Information Security Measures te automatiseren in het softwareontwikkelproces.

De doelstelling van dit onderzoek is het bepalen van welke Information Security Measures geautomatiseerd kunnen worden in het Continuous Delivery softwareontwikkelproces.
Indien de Information Security Measures geautomatiseerd worden in een Deployment Pipeline, kan bij elke fase dat doorlopen wordt in een Deployment Pipeline, geautomatiseerd bewijslast opgeleverd worden. Hiermee wordt het probleem met handmatig werk, zoals het verzamelen van bewijsmateriaal, zoveel mogelijk opgelost. Het automatisch verzamelen van bewijsmateriaal zal uiteindelijk gaan leiden naar Continuous Compliance.

Om te bepalen welke Information Security Measures geautomatiseerd kunnen worden in een Deployment Pipeline zullen de onderstaande vragen in zowel het literatuur- en het empirisch onderzoek onderzocht worden.

Centrale vraag:
Welke Information Security Measures kunnen geautomatiseerd worden binnen de Continuous Deployment Pipeline zodat een Continuous Compliance framework bewerkstelligd kan worden?

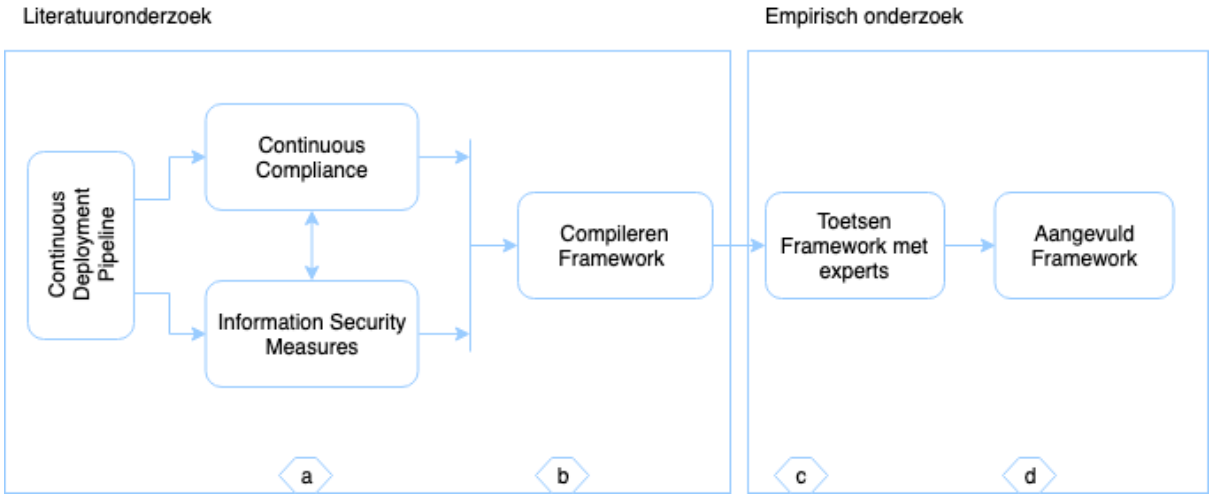
Deelvragen voor zowel literatuur- als empirisch onderzoek:
1. Wat is een bruikbaar framework voor Continuous Compliance?
2. Welke Information Security Frameworks worden veelal gebruikt binnen een Continuous Deployment Pipeline?
3. Welke Information Security Measures kunnen gesteld worden aan een Continuous Deployment Pipeline?
4. Welke Information Security Measures kunnen eenvoudig geautomatiseerd worden in een Continuous Deployment Pipeline?

Het beantwoorden van deelvraag één zal inzicht geven in reeds bestaande frameworks voor Continuous Compliance. Indien in de wetenschappelijke literatuur al bruikbare Continuous Compliance frameworks bestaan, zal het antwoord op de centrale vraag wellicht al gegeven kunnen worden. Deelvraag twee zal inzicht geven of bestaande Information Security Frameworks al toegepast worden op Continuous Deployment Pipelines. Indien er al een aantal Frameworks gebruikt worden, kan het bepalen van welke Information Security Measures geautomatiseerd kunnen worden eenvoudiger worden. Het antwoord op de derde deelvraag zal de centrale vraag ondersteunen door inzicht te geven in wat voor soort Information Security Measures belangrijk zijn om te stellen aan Deployment Pipelines. Deelvraag vier zal inzicht geven in welke Information Security Measures ‘eenvoudig’ geautomatiseerd kunnen worden in een Deployment Pipeline en uiteindelijk de centrale vraag beantwoorden met een duidelijke lijst dat inzichtelijk maakt welke Information Security Measures op een eenvoudige manier geautomatiseerd kunnen worden.

1.6. Aanpak in hoofdlijnen

Dit afstudeeronderzoek wordt uitgevoerd in het kader van het afstuderen voor de masteropleiding Business Process Management & Information and Technology aan de Open Universiteit Nederland. In het volgende hoofdstuk zal de onderzoeksaanpak voor deze literatuurstudie beschreven worden die met behulp van een onderzoeksmodel ook zal worden ondersteund. Vervolgens zal naar aanleiding van de gestelde onderzoeksvragen in wetenschappelijke literatuur gezocht worden naar de antwoorden. Op basis van de verkregen antwoorden vanuit de literatuur zal een theoretisch model opgesteld worden dat een basis gaat vormen voor het uitvoeren van het empirisch onderzoek, zie figuur 2.

Het doel van dit afstudeeronderzoek is om een model te construeren dat inzicht geeft in welke Information Security Measures geautomatiseerd kunnen worden binnen een Continuous Deployment Pipeline. Het model zal in het empirisch onderzoek getoetst en aangevuld worden zodat er een aangevuld model ontstaat. De opzet van dit onderzoek is hieronder weergegeven in een onderzoeksmodel dat op basis van theorieën van Verschuren & Doorewaard (2007) is opgesteld.



Figuur 2: Aanpak onderzoeksmodel

In de eerste fase (a) zijn de kernconcepten van de bestaande begrippen onderzocht. In fase (b) is op basis van theorie dat gevonden is in fase (a) een framework gecompileerd in de vorm van een vragenlijst dat gebaseerd is op het ISF framework (bijlage 4). Dit framework fungeert als startpunt voor het empirisch onderzoek en zal ook de centrale vraag beantwoorden. In fase (c) is het framework samen met experts getoetst met een verkennend onderzoek waarin de experts hebben aangegeven in welke mate van eenvoudigheid de Information Security Measures te automatiseren zijn in een Deployment Pipeline. Vervolgens is het framework op basis van de semi-gestructureerde interviews in fase (d) verder aangevuld. Op basis van de gegeven antwoorden op de deelvragen is onder andere een definitie gedestilleerd voor Continuous Compliance waarmee het framework (bijlage 6) verder is aangevuld.

2. Theoretisch kader

In dit hoofdstuk wordt beschreven welke zoekstrategie is gehanteerd om relevante literatuur te vinden zodat de centrale vraag beantwoord kan worden. Naar aanleiding van de gevonden literatuur worden de resultaten en conclusies toegelicht waarna dit hoofdstuk wordt afgesloten met het doel van het vervolgonderzoek.

2.1. Onderzoeksaanpak

In deze paragraaf wordt het doel en de opzet van het theoretisch kader beschreven.

2.1.1. Doel literatuuronderzoek

Doel van het literatuuronderzoek is om antwoord te krijgen op de centrale vraag: Welke Information Security Measures kunnen worden geautomatiseerd én geïntegreerd binnen de Continuous Deployment Pipeline zodat Continuous Compliance bewerkstelligd kan worden?

Om deze vraag te beantwoorden is er een aantal deelvragen opgesteld. Binnen dit hoofdstuk wordt er getracht om vanuit de wetenschappelijke literatuur antwoord te vinden op deze deelvragen.

2.1.2. Aanpak literatuuronderzoek

Het literatuuronderzoek is opgezet op basis van Systematic Literature Review (SLR) wat volgens Shahin, Babar, & Zhu (2017) de meest gebruikte onderzoeksmethode is in “Evidence Based Software Engineering”. Volgens de onderzoekers heeft SLR het doel een goed gedefinieerd proces te bieden voor het identificeren, evalueren en interpreteren van alle beschikbare gegevens die relevant zijn voor een specifieke onderzoeksvraag of onderwerp.

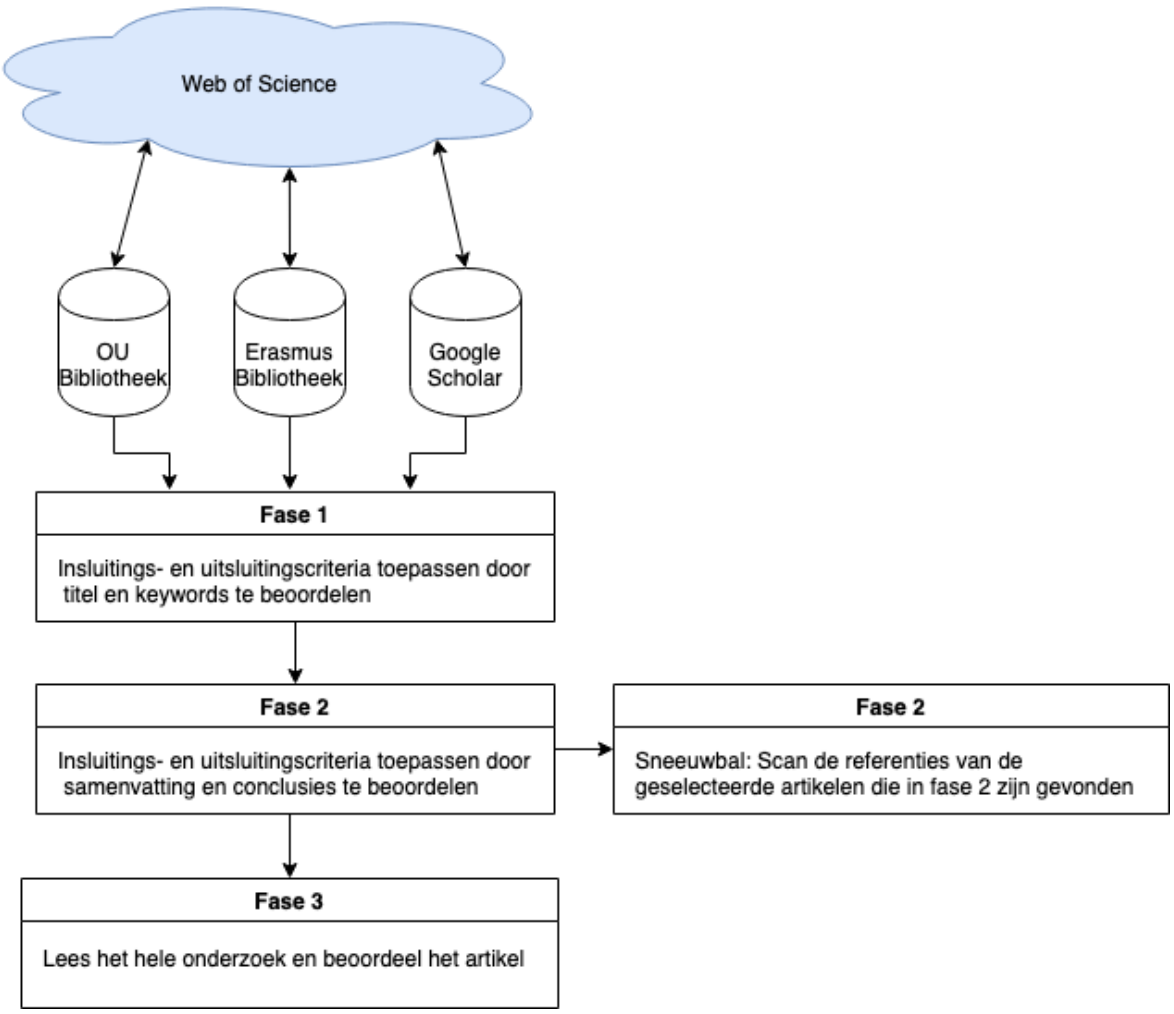
Om de deelvragen te kunnen beantwoorden is gezocht naar relevante peer-reviewed publicaties. Tevens is naar relevante literatuur gezocht om in het vooronderzoek de inleiding en de probleemstelling waar mogelijk wetenschappelijk te onderbouwen.

Tijdens het zoeken naar literatuur is voornamelijk gebruik gemaakt van systematisch zoeken door op basis van gecombineerde zoektermen in zoekmachines te zoeken en de sneeuwbalmethode door artikelen te zoeken die als referentie zijn gebruikt in de gevonden artikelen. Tevens zijn tijdens het zoeken gebruik gemaakt van bepaalde zoektechnieken zoals;

- boole-logica om gecombineerd te zoeken of uit te sluiten met AND, OR, NOT
- exact phrase, om het zoeken op exacte woordcombinatie mogelijk te maken
- veldspecifiek, zoeken op titel en/of samenvatting

Doordat de meeste publicaties en de termen zelf in het Engels zijn is voornamelijk gezocht met Engelse zoektermen. Om de gevonden artikelen te sorteren en te categoriseren is gebruik gemaakt van EndNote.

Om de gevonden zoekresultaten tot een behapbare selectie terug te dringen is het zoekproces in het figuur hieronder gevolgd.



Figuur 3: Fases van het zoekproces

Tevens is een aparte literatuurlijst op een systematische manier bijgehouden met de gebruikte zoektermen, datum van raadplegen, titel van artikel, auteur(s), jaar van publicatie, relevantie van het artikel, in welke bron het artikel is gevonden, URL naar de bron etc. Deze lijst is terug te vinden als bijlage 1.

In het kader van volledigheid is vertrokken vanuit de lijst op Wikipedia (frame of reference) van officiële Information Science Research Journals. Vervolgens zijn de zoektermen gedefinieerd en zijn de zoekopdrachten uitgevoerd binnen de bibliotheek van de Open Universiteit, Erasmus en Google Scholar. Met dien verstande dat deze drie bibliotheken voldoende toegang verschaffen tot de volledige lijst met relevante literatuur. Aan het eind van het literatuuronderzoek is een volledigheidscheck gedaan of de geraadpleegde bronnen in de "List of Computer Science Journals," (2019) voorkomen.

2.1.3. Zoektermen

De volgende zoektermen zijn gebruikt om relevante literatuur te vinden om de inleiding en probleemstelling wetenschappelijk te onderbouwen:

Demanding customers, veeleisende klanten, spreadsheets, auditing, spreadsheet auditing, continuous delivery, continuous compliance, compliance, regulations, laws, policies, internal control, corporate governance.

In onderstaand tabel worden de zoektermen en de rationale erachter getoond. Deze zoektermen zijn gebruikt om op een systematische manier relevante literatuur te vinden met als doel de deelvragen te beantwoorden.

Zoekterm	Rationale
Continuous Compliance Framework(s)	Onderzoeken die een framework beschrijven die toegepast kunnen worden om Continuous Compliance te bewerkstelligen in de context van Continuous Delivery
Information Security Framework(s)	Onderzoeken die Information Security Frameworks beschrijven die toegepast kunnen worden in Continuous Delivery, Continuous Deployment en Cloud omgevingen
Continuous Deployment Pipeline(s)	Onderzoeken die over Continuous Deployment Pipelines gaan in de context van Information Security Frameworks, Security Automation, Information Security Controls en Information Security Measurres
Continuous Delivery	Onderzoeken die over de "Continuous Delivery" gaan in de context van Information Seurity Measures en information Security Controls
Cloud	Onderzoeken die over de "Cloud" gaan in de context van Information Seurity Measures en information Security Controls
Information Security Measures	Onderzoeken die over Information Security Measures gaan in de context Continuous Delivery, Continuous Deployment Pipelines en Cloud
Information Security Controls	Onderzoeken die over Information Security Controls gaan in de context context Continuous Delivery, Continuous Deployment Pipelines en Cloud
Security Automation	Onderzoeken die over "Security Automation" gaan in de context van Information Security Measures, Information Security Controls, Continuous Deployment Pipelines en Cloud

Tabel 1: Zoektermen die gehanteerd zijn tijdens het literatuuronderzoek

Om het risico te beperken dat relevante onderzoeken gemist worden, zijn tijdens het zoeken in de verschillende databanken deze zoektermen op verschillende manieren gecombineerd.

2.1.4. Zoekbronnen

De volgende zoekmachines zijn gebruikt om relevante literatuur te vinden:

- Digitale bibliotheek van de Open Universiteit
- Digitale bibliotheek van de Erasmus Universiteit
- Google Scholar

De zoektermen zijn altijd in minimaal twee primaire zoekmachines gezocht, bijvoorbeeld Google Scholar is altijd in combinatie gebruikt met één van de universiteitsbibliotheken.

2.1.5. Selectieproces

In deze sub paragraaf wordt beschreven welke criteria zijn gehanteerd om te komen tot een lijst met relevante literatuur.

Om een eerste selectie te maken zijn de volgende criteria gehanteerd:

- Artikelen die geen peer-reviewed wetenschappelijke artikelen waren of boeken, hoofdstukken van boeken zijn uitgesloten
- Artikelen die niet gerelateerd waren aan het IT-domein zijn uitgesloten (zoals bijv. health, medicine, drugs, meteorological, etc.)
- Continuous Delivery en Continuous Compliance zijn begrippen die ook veel voorkomen in de medische industrie. De meest voorkomende begrippen in deze industrie, zoals health, medical, medicine, etc., zijn eruit gefilterd bij het zoeken naar relevante literatuur.
- Niet Engelstalige artikelen zijn uitgesloten
- Voor de begrippen Continuous Deployment Pipeline en Continuous Compliance zijn alleen artikelen geselecteerd vanaf 2010 omdat deze concepten zijn ontstaan nadat het boek van Humble & Farley (2010) is verschenen. Dit boek wordt zowel in de wetenschap als in praktijk als concept bepalend gebruikt.

Om de artikelen inhoudelijk te beoordelen zijn de volgende criteria gehanteerd:

- Komt de titel en de keywords overeen met de zoektermen?
- Geeft het gevonden artikel antwoord op de gestelde deelvraag?
    - In eerste instantie is de samenvatting, vervolgens de introductie en conclusie gelezen en daarna pas het hele artikel
- Komen de begrippen die binnen de andere deelvragen worden gesteld ook aan bod? Als het artikel relevant is bevonden voor een andere deelvraag is dit in de kolom “Aantekeningen” aangegeven in bijlage 1
- Is de data binnen het onderzoek verkregen vanuit wetenschappelijk onderzoek?
- Zijn de referenties die de onderzoekers gebruiken peer-reviewed?
- Zijn de onderzoekers onafhankelijk? Zijn ze bijvoorbeeld een specifieke tool aan het promoten binnen hun artikel?

In de volgende paragraaf is een overzicht opgenomen van de geselecteerde en niet geselecteerde bronnen.

2.2. Uitvoering literatuuronderzoek

In deze paragraaf wordt kort beschreven hoe het literatuuronderzoek is verlopen, hoeveel artikelen zijn gevonden, hoeveel daarvan relevant waren voor dit literatuuronderzoek en hoe die tot een beheersbare hoeveelheid zijn teruggebracht.

2.2.1. Continuous Compliance Framework

Om de eerste deelvraag *'Wat is een bruikbaar framework voor Continuous Compliance?'* te kunnen beantwoorden zijn de volgende zoekkaders gebruikt.

Stap	Zoekbron	Zoekterm	Zoekkader	Resultaten
1	OU Bibliotheek	continuous compliance	Titel	303
2	OU Bibliotheek	continuous compliance	Titel + sinds 01-01-2010	212
3	OU Bibliotheek	continuous compliance	Titel + sinds 01-01-2010 + Scholarly & Peer-Review	103
4	OU Bibliotheek	continuous compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	10
1	OU Bibliotheek	continuous compliance framework	Titel	3
2	OU Bibliotheek	continuous compliance framework	Titel + sinds 01-01-2010	2
3	OU Bibliotheek	continuous compliance framework	Titel + sinds 01-01-2010 + Scholarly & Peer-Review	0
4	OU Bibliotheek	continuous compliance framework	Samenvatting	161
5	OU Bibliotheek	continuous compliance framework	Samenvatting + sinds 01-01-2010 + Peer-Reviewed	80
6	OU Bibliotheek	continuous compliance framework	Samenvatting + sinds 01-01-2010 + Peer-Reviewed (Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	26
1	Google Scholar	continuous compliance framework	Titel + sinds 01-01-2010 allintitle: continuous compliance framework -drug -medical -medicine -patients -health	1
			Totaal	37

Tabel 2: Zoekresultaten deelvraag 1

Deze zoekopdracht is voor het laatst uitgevoerd op 6 juli 2019.

De 37 gevonden resultaten zijn op een systematische manier in een lijst bijgehouden. De volledige lijst is in bijlage 1 weergegeven. Sommige begrippen in de medische branche en in de IT branche komen overeen maar hebben een andere lading, daarom zijn deze begrippen uitgesloten in de zoekopdrachten.

In eerste instantie zijn de gevonden artikelen beoordeeld op de titel daarna op samenvatting en inhoud. Als het aan de titel niet duidelijk te herleiden was waar het artikel over ging is eerst de

samenvatting gelezen. Indien in de samenvatting mogelijke aanknopingspunten zijn geconstateerd, is de inhoud beoordeeld. Bij de tweede zoekterm, “continuous compliance framework” is bewust gezocht in de samenvatting omdat de zoekresultaten in de titel niets opgeleverd heeft. In totaal zijn er drie artikelen gevonden die op inhoud beoordeeld zijn. In bijlage 1 is de lijst opgenomen met de artikelen die beoordeeld zijn op inhoud.

In paragraaf 2.3.1. zijn de resultaten van het literatuuronderzoek beschreven.

2.2.2. Information Security Frameworks in Deployment Pipelines

Om de tweede deelvraag *'Welke Information Security Frameworks worden veelal gebruikt binnen een Continuous Deployment Pipeline?'* te beantwoorden zijn de volgende zoekkaders gebruikt.

#	Zoekbron	Zoekterm	Zoekkader	Resultaten
1	Google Scholar	Information Security Frameworks	allintitle: Information Security Framework, sinds 2010	363
2	Google Scholar	Information Security Framework	allintitle: Information Security Framework, sinds 2010	33
3	Google Scholar	Information Security Framework(s) AND Deployment Pipeline(s)	allintitle: Information Security Framework(s) Deployment Pipeline(s), sinds 2010	0
4	Google Scholar	Security Framework(s) AND Deployment Pipelines	allintitle: Security Frameworks Deployment Pipelines, sinds 2010	0
5	Google Scholar	Security Framework(s) AND Continuous Deployment	allintitle: Security Frameworks Continuous Deployment, sinds 2010	0
6	Google Scholar	Security Framework(s) AND Continuous Delivery	allintitle: Security Frameworks Continuous Delivery, sinds 2010	0
7	Google Scholar	Information Security AND Continuous Delivery	allintitle: Information Security Continuous Delivery, sinds 2010	0
8	Google Scholar	Information Security Frameworks	allintitle: Information Security Frameworks, sinds 2010	39
9	Google Scholar	Information Security Frameworks AND Cloud	allintitle: Information Security Frameworks Cloud, sinds 2010	7
10	Google Scholar	Information Security Framework AND Cloud	allintitle: Information Security Framework Cloud, sinds 2010	23
11	Erasmus bibliotheek	Information Security Frameworks	Titel + sinds 2010, Peer-Reviewed, Engels ti:(Information Security Frameworks)	159
12	Erasmus bibliotheek	Information Security Framework	Titel + sinds 2010, Peer-Reviewed, Engels ti:(Information Security Framework)	159
13	Erasmus bibliotheek	Information Security Framework(s) AND Deployment Pipeline(s)	Titel ti:(Information Security Frameworks) AND Deployment Pipelines) ti:(Information Security Framework) AND Deployment Pipeline) ti:(Information Security Frameworks) AND Deployment Pipeline) ti:(Information Security Frameworks) AND Deployment Pipelines)	0
14	Erasmus bibliotheek	Information Security Framework(s) AND Continuous Deployment	Titel ti:(Information Security Frameworks) AND Continuous Deployment ti:(Information Security Framework) AND Continuous Deployment	0
15	Erasmus bibliotheek	Information Security Framework(s) AND Continuous Delivery	Titel ti:(Information Security Frameworks) AND Continuous Delivery ti:(Information Security Framework) AND Continuous Delivery	0
16	Erasmus bibliotheek	Information Security Framework(s) AND Cloud	Titel + sinds 2010, Peer-Reviewed, Engels ti:(Information Security Frameworks) AND ti:(cloud) ti:(Information Security Framework) AND ti:(cloud)	20
17	Erasmus bibliotheek	Information Security Framework(s) AND Deployment Pipeline(s)	Samenvatting + Peer-Reviewed ab:(Information security framework) AND ab:(deployment pipeline) ab:(Information security frameworks) AND ab:(deployment pipelines) ab:(Information security frameworks) AND ab:(deployment pipeline) ab:(Information security frameworks) AND ab:(deployment pipelines)	0
18	Erasmus bibliotheek	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels ab:(Information security frameworks) AND ab:(continuous deployment) ab:(Information security framework) AND ab:(continuous deployment)	9
19	Erasmus bibliotheek	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels ab:(Information security framework) AND ab:(continuous delivery) ab:(Information security frameworks) AND ab:(continuous delivery)	13
			Totaal	72

Tabel 3: Zoekresultaten deelvraag 2

Deze zoekopdracht is voor het laatst uitgevoerd op 31 juli 2019.

De 72 gevonden resultaten zijn op een systematische manier in een lijst bijgehouden. De volledige lijst is in bijlage 1 opgenomen.

In eerste instantie zijn de gevonden artikelen beoordeeld op de titel daarna op samenvatting en inhoud. Als het aan de titel niet duidelijk te herleiden was waar het artikel over ging is eerst de samenvatting gelezen. Indien in de samenvatting mogelijke aanknopingspunten zijn geconstateerd, is de inhoud beoordeeld. Bij het zoeken naar het woord 'Frameworks' en 'Pipeline' is er rekening gehouden met meervoudige en enkelvoudige zoektermen. De term Information Security Framework(s) levert veel resultaten op, echter is in deze zoekopdracht de combinatie belangrijk. Om deze reden zijn alleen de artikelen doorgenomen die twee of meer zoektermen bevatten. De zoekresultaten met Continuous Delivery, Continuous Deployment, Deployment Pipeline in combinatie met Information Security Framework(s) hebben niets opgeleverd. Om deze reden zijn deze termen vervangen met 'Cloud' ervan uitgaande dat Continuous Delivery projecten en Deployment Pipelines veelal in de Cloud worden gebruikt.

Sommige zoektermen hebben in de titel niets opgeleverd, daarom is gezocht naar de combinatie in de samenvattingen. In totaal zijn 17 artikelen beoordeeld op de inhoud. In bijlage 1 is de lijst opgenomen met de artikelen die beoordeeld zijn op inhoud.

In paragraaf 2.3.2. zijn de resultaten van het literatuuronderzoek beschreven.

2.2.3. Information Security Measures in Deployment Pipelines

Om de derde deelvraag *'Welke Information Security Measures kunnen gesteld worden aan een Continuous Deployment Pipeline?'* te kunnen beantwoorden zijn de zoekkaders gebruikt die in deze paragraaf zijn opgenomen.

De zoekresultaten hebben 44 resultaten opgeleverd waarvan 13 artikelen inhoudelijk zijn beoordeeld. In bijlage 1 is de lijst opgenomen met de artikelen die beoordeeld zijn op inhoud. In paragraaf 2.3.3. zijn de resultaten van de relevant bevonden artikelen uit het literatuuronderzoek uitgewerkt. In eerste instantie zijn de gevonden artikelen beoordeeld op de titel daarna op samenvatting en inhoud. Als het aan de titel niet duidelijk te herleiden was waar het artikel over ging is eerst de samenvatting gelezen. Indien in de samenvatting mogelijke aanknopingspunten zijn geconstateerd, is de inhoud beoordeeld.

Hieronder wordt in tabel 4 getoond hoeveel resultaten er zijn gevonden met de gegeven zoekkaders. Met blauw gearceerde resultaten zijn in eerste instantie op titel daarna op inhoud beoordeeld. De dik gedrukte regels zijn de zoekkaders die de resultaten hebben opgeleverd. Bij het zoeken naar artikelen is rekening gehouden met zoektermen in enkelvoud of meervoud.

De zoekresultaten met Continuous Delivery, Continuous Deployment, Deployment Pipeline in combinatie met Information Security Measures en Controls hebben weinig tot niets opgeleverd. Ook hier is gekozen om deze termen te vervangen met 'Cloud' ervan uitgaande dat Continuous Delivery projecten en Deployment Pipelines veelal in de Cloud worden gebruikt. Bij de zoekterm 'Cloud' kwamen er ook artikelen over het klimaat naar voren, deze termen zijn weggelaten bij het zoeken naar relevante artikelen.

#	Zoekbron	Zoekterm	Zoekkader	Resultaten
1	Google Scholar	Information Security Measures AND Continuous Deployment Pipeline(s)	Titel, sinds 2010 allintitle: Information Security Measures Continuous Deployment Pipeline allintitle: Security Measures Continuous Deployment Pipeline **allintitle: Security Continuous Deployment Pipeline** allintitle: Measures Continuous Deployment Pipeline	1
2	Google Scholar	Information Security Controls AND Continuous Deployment Pipeline(s)	Titel, sinds 2010 allintitle: Information Security Controls Continuous Deployment Pipeline allintitle: Security Controls Continuous Deployment Pipeline allintitle: Controls Continuous Deployment Pipeline	0
3	Google Scholar	Information Security Measures AND Continuous Delivery	Titel, sinds 2010 allintitle: Information Security Measures Continuous Delivery allintitle: Security Measures Continuous Delivery allintitle: Measures Continuous Delivery **allintitle: Security Continuous Delivery**	2
4	Google Scholar	Information Security Controls AND Continuous Delivery	Titel, sinds 2010 allintitle: Information Security Controls Continuous Delivery allintitle: Security Controls Continuous Delivery allintitle: Controls Continuous Delivery	0
5	Google Scholar	Information Security measures AND Cloud	Titel, sinds 2010 allintitle: information security measures cloud	4
6	Google Scholar	Information Security Controls AND Cloud	Titel, sinds 2010 allintitle: information security controls cloud	0
7	Erasmus bibliotheek	Information Security Measures AND Continuous Deployment Pipeline(s)	Titel ti:(Information Security Measures) AND ti:(Continuous Deployment Pipelines) ti:(Security Measures) AND ti:(Continuous Deployment Pipelines) ti:(Security) AND ti:(Continuous Deployment Pipelines) ti:(Measures) AND ti:(Continuous Deployment Pipeline) ti:(Information Security Measures) AND ti:(Deployment Pipelines) ti:(Information Security Measures) AND ti:(Deployment Pipelines) ti:(Security) AND ti:(Deployment Pipelines) ti:(Measures) AND ti:(Deployment Pipelines)	0
8	Erasmus bibliotheek	Information Security Controls AND Continuous Deployment Pipeline(s)	Titel ti:(Information Security Controls) AND ti:(Continuous Deployment Pipelines) ti:(Security Controls) AND ti:(Continuous Deployment Pipelines) ti:(Controls) AND ti:(Continuous Deployment Pipelines) ti:(Information Security Controls) AND ti:(Deployment Pipelines) ti:(Information Security Controls) AND ti:(Deployment Pipelines) **ti:(Controls) AND ti:(Deployment Pipelines)**	1
9	Erasmus bibliotheek	Information Security Measures AND Continuous Delivery	Titel, sinds 2010, Peer-Reviewed ti:(Information Security Measures) AND ti:(Continuous Delivery) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:(Security Measures) AND ti:(Continuous Delivery) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:(Security) AND ti:(Continuous Delivery) AND (eu:Peerreviewed) AND (yr:2010..2019) **ti:(Measures) AND ti:(Continuous Delivery) AND (eu:Peerreviewed) AND (yr:2010..2019) NOT ti:(health)**	1
10	Erasmus bibliotheek	Information Security Controls AND Continuous Delivery	Titel, sinds 2010, Peer-Reviewed ti:(Information Security Controls) AND ti:(Continuous Delivery) NOT ti:(health) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:(Security Controls) AND ti:(Continuous Delivery) NOT ti:(health) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:(Controls) AND ti:(Continuous Delivery) NOT ti:(health) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Controls" AND ti:"Continuous Delivery" NOT ti:(health) AND (eu:Peerreviewed) AND (yr:2010..2019)	0
11	Erasmus bibliotheek	Information Security Measures AND Continuous Deployment Pipeline(s)	Samenvatting, sinds 2010, Peer-Reviewed ab:(Information Security Measures) AND ab:(Continuous Deployment Pipeline) AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Security Measures) AND ab:(Continuous Deployment Pipeline) AND (eu:Peerreviewed) AND (yr:2010..2019) **ab:(Security) AND ab:(Continuous Deployment Pipeline) AND (eu:Peerreviewed) AND (yr:2010..2019)** ab:(Information Security Measures) AND ab:(Deployment Pipeline) AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Security Measures) AND ab:"Deployment Pipeline" AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Measures) AND ab:"Deployment Pipeline" AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Security) AND ab:"Deployment Pipeline" AND (eu:Peerreviewed) AND (yr:2010..2019)	1
12	Erasmus bibliotheek	Information Security Controls AND Continuous Deployment Pipeline(s)	Samenvatting, sinds 2010, Peer-Reviewed ab:(Information Security Controls) AND ab:(Continuous Deployment Pipeline) AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Security Controls) AND ab:"Continuous Deployment Pipeline" AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Controls) AND ab:"Continuous Deployment Pipeline" AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Information Security Controls) AND ab:(Deployment Pipeline) AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Security Controls) AND ab:(Deployment Pipeline) AND (eu:Peerreviewed) AND (yr:2010..2019) ab:(Controls) AND ab:"Deployment Pipeline" AND (eu:Peerreviewed) AND (yr:2010..2019)	2
13	Erasmus bibliotheek	Information Security Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed ti:"Information Security Measures" AND ti:"Cloud" AND (eu:Peerreviewed) AND (yr:2010..2019) **ti:"Security Measures" AND ti:"Cloud" AND (eu:Peerreviewed) AND (yr:2010..2019)** **ti:"Measures" AND ti:"Cloud" AND (eu:Peerreviewed) AND (yr:2010..2019)**	17
14	Erasmus bibliotheek	Information Security Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed ti:"Information Security Controls" AND ti:"Cloud" AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Security Controls" AND ti:"Cloud" AND (eu:Peerreviewed) AND (yr:2010..2019) **ti:"Controls" AND ti:"Cloud" AND (eu:Peerreviewed) AND (yr:2010..2019) NOT kf:(water) NOT kf:(climate)**	15
			Totaal	**44**

Tabel 4: Zoekresultaten Deelvraag 3

In bijlage 1 is de volledige lijst met zoekresultaten opgenomen. De zoekopdracht is meerdere malen uitgevoerd, voor het laatst is er gezocht op 31 juli 2019.

2.2.4. Automatisering van Information Security Measures

Om de vierde deelvraag *'Welke Information Security Measures kunnen eenvoudig geautomatiseerd worden in een Continuous Deployment Pipeline?'* te kunnen beantwoorden zijn de zoekkaders gebruikt die in deze paragraaf zijn opgenomen.

De zoekresultaten hebben 33 resultaten opgeleverd waarvan 10 artikelen inhoudelijk zijn beoordeeld. In bijlage 1 is de lijst opgenomen met de artikelen die beoordeeld zijn op inhoud. In paragraaf 2.3.4. zijn de resultaten van de relevant bevonden artikelen uit het literatuuronderzoek uitgewerkt.

Hieronder wordt in tabel 5 getoond hoeveel resultaten er zijn gevonden met de gegeven zoekkaders. Met blauw gearceerde resultaten zijn in eerste instantie op titel daarna op inhoud beoordeeld. De dik gedrukte regels zijn de zoekkaders die de resultaten hebben opgeleverd. Tevens is bij het zoeken naar artikelen rekening gehouden met zoektermen in enkelvoud of meervoud.

#	Zoekbron	Zoekterm	Zoekkader	Resultaten
1	Google Scholar	Information Security Measures AND Automation	Titel, sinds 2010 allintitle: Information Security Measures Automation allintitle: Information Security Measures Automated **allintitle: "Security Measures" Automation** **allintitle: "Security Measures" Automated**	3
2	Google Scholar	Information Security Controls AND Automation	Titel, sinds 2010 allintitle: "Information Security Controls" Automation **allintitle: "Information Security Controls" Automated** **allintitle: "Security Controls" Automation** **allintitle: "Security Controls" Automated**	4
3	Google Scholar	Automation AND Continuous Deployment Pipeline	Titel, sinds 2010 allintitle: Automation Continuous Deployment Pipeline **allintitle: Automated Continuous Deployment Pipeline** allintitle: Automation Deployment Pipeline **allintitle: Automated Deployment Pipeline**	2
4	Google Scholar	Security Automation AND Continuous Deployment Pipeline	Titel, sinds 2010 allintitle: Security Automation Continuous Deployment Pipeline allintitle: Security Automation Deployment Pipeline	0
5	Google Scholar	Security Automation AND Continuous Delivery	Titel, sinds 2010 allintitle: Security Automation Continuous Delivery **allintitle: Automation Continuous Delivery** **allintitle: Automated Continuous Delivery**	13
6	Erasmus Bibliotheek	Information Security Measures AND Automation	Titel, sinds 2010, Peer-Reviewed ti:(Information Security Measures) AND ti:(Automation) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Information Security Measures" AND ti:(Automated) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Security Measures" AND ti:(Automation) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Security Measures" AND ti:(Automated) AND (eu:Peerreviewed) AND (yr:2010..2019)	0
7	Erasmus Bibliotheek	Information Security Controls AND Automation	Titel, sinds 2010, Peer-Reviewed **ti:(Information Security Controls) AND ti:(Automation) AND (eu:Peerreviewed) AND (yr:2010..2019)** **ti:"Information Security Controls" AND ti:(Automated) AND (eu:Peerreviewed) AND (yr:2010..2019)** **ti:"Security Controls" AND ti:(Automation) AND (eu:Peerreviewed) AND (yr:2010..2019)** **ti:"Security Controls" AND ti:(Automated) AND (eu:Peerreviewed) AND (yr:2010..2019)**	10
8	Erasmus Bibliotheek	Automation AND Continuous Deployment Pipeline	Titel, sinds 2010, Peer-Reviewed ti:"Continuous Deployment Pipeline" AND ti:(Automation) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Continuous Deployment Pipeline" AND ti:(Automated) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Deployment Pipeline" AND ti:(Automation) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:"Deployment Pipeline" AND ti:(Automated) AND (eu:Peerreviewed) AND (yr:2010..2019)	0
9	Erasmus Bibliotheek	Security Automation AND Continuous Delivery	Titel, sinds 2010, Peer-Reviewed ti:(Continuous Delivery) AND ti:(Security Automation) AND (eu:Peerreviewed) AND (yr:2010..2019) ti:(Continuous Delivery) AND ti:(Security Automated) AND (eu:Peerreviewed) AND (yr:2010..2019) **ti:(Continuous Delivery) AND ti:(Automation) AND (eu:Peerreviewed) AND (yr:2010..2019)**	1
			Totaal	**33**

Tabel 5: Zoekresultaten deelvraag 4

In Bijlage 1 is de volledige lijst met zoekresultaten opgenomen. De zoekopdracht is meerdere malen uitgevoerd, voor het laatst is er gezocht op 31 juli 2019.

2.3. Resultaten en conclusies

In deze paragraaf worden de resultaten, die voor zover zijn gevonden uit het literatuuronderzoek, beschreven. De resultaten uit het literatuuronderzoek zijn in sub-paragrafen uitgeschreven. Na de verwerking van de resultaten is ook een conclusie geschreven van het theoretisch kader.

2.3.1. Continuous Compliance Framework

In deze paragraaf wordt naar aanleiding van het literatuuronderzoek getracht antwoord te geven op de eerste deelvraag:

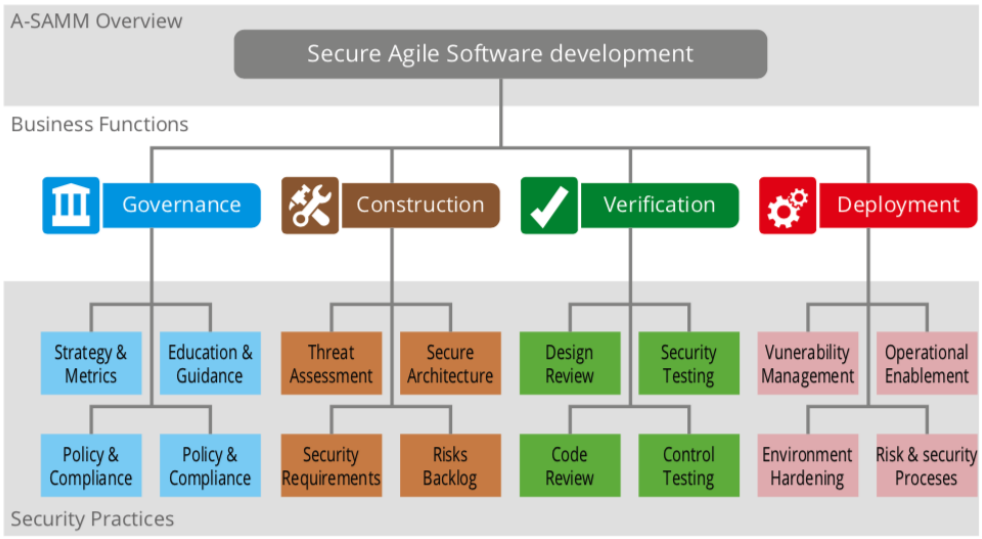
Wat is een bruikbaar framework voor Continuous Compliance?

Li, Jin, Wang, Cao, & Chen (2018) geven in hun onderzoek aan dat Internet of Things (IoT) veel security en compliance problemen met zich meebrengt. Om dit probleem op te lossen hebben ze in hun onderzoek een voorstel gedaan voor een secure en compliant continu assessment framework (SCCAF). Dit framework kan gebruikt worden om de security- en compliance niveaus van cloud services in life-cycle te evalueren. De SCCAF faciliteert een cloud service aan klanten om een optimale Cloud Service Provider (CSP) te selecteren die voldoet aan hun gewenste beveiligingsvereisten. Dit framework focust zich op Internet of Things (IoT) en voornamelijk op de fysieke laag en is daarom niet bruikbaar voor dit onderzoek. Het onderzoek van Li et al. (2018) geeft geen antwoord op de gestelde deelvraag.

Vedani & Ramaharobandro (2013) hebben een Continuous Compliance framework gemaakt dat gebaseerd is op Solvency II. Solvency II is een toezichtsraamwerk voor verzekeraars en voornamelijk gericht op processen en procedures. Dit Continuous Compliance framework zegt niets over Continuous Delivery of Continuous Deployment Pipeline en geeft daarom ook geen antwoord op de gestelde deelvraag.

In de wetenschappelijke literatuur is geen duidelijke definitie gevonden van Continuous Compliance in context van Continuous Delivery.

Derksen, Neggers, Onwezen, & Zelen (2018) hebben in hun boek *'Agile Secure Software Lifecycle Management Secure by Agile Design'* een model beschreven dat dicht bij het concept van Continuous Compliance in de buurt komt. Het model heet Agile Software Assurance Maturity Model (ASAMM) en is gebaseerd op Software Assurance Maturity Model "OpenSAMM," (2019). SAMM is een open framework dat in 2009 is ontwikkeld. ASAMM is een aanvulling hierop en focust zich meer op secure agile software ontwikkeling.



Figuur 4: Agile Software Assurance Maturity Model (ASAMM, copyright SSA).

In de ASAMM is het bestaande SAMM model aangevuld met: Risks Backlog, Control Testing en Risk & Security Processes. Met deze aanvullingen kan dit model als goede basis gebruikt worden voor een Continuous Compliance framework. Dit boek is beperkt wetenschappelijk onderbouwd en daarom wordt het in dit onderzoek niet opgenomen als relevante bron voor een Continuous Compliance Framework.

2.3.2. Information Security Frameworks in Deployment Pipelines

In deze paragraaf wordt getracht antwoord te geven naar aanleiding van het literatuuronderzoek op de tweede deelvraag:

Welke Information Security Frameworks worden veelal gebruikt binnen een Continuous Deployment Pipeline?

Rebollo, Mellado, & Fernández-Medina (2012) hebben onderzocht welke verschillende Information Security Governance (ISG) Frameworks gebruikt kunnen worden in de Cloud Computing. De onderzoekers geven in hun onderzoek aan dat de vergelijkingsresultaten aantonen dat de meeste van de beoordeelde ISG-frameworks gedeeltelijk omgaan met alle voorgestelde cloud security criteria, maar dat extra inspanningen moeten worden geleverd om de gedetecteerde hiaten op te vullen. Om een alomvattende ISG-aanpak te bereiken die geschikt is voor een Cloud Computing-omgeving, moeten de tekortkomingen van te voren worden beoordeeld en opgelost voordat de service wordt geïmplementeerd. Een overzicht van de frameworks die Rebollo et al. (2012) hebben behandeld is opgenomen in Tabel 6.

Volgens Alnuem, Alrumaih, & Al-Alshaikh (2015) is het uitvoeren van een information security risk management het kernelement van een Information Security Management System (ISMS). ISO 27001 is de internationale best practice standard voor ISMS. ISO / IEC 27000 biedt beleid, normen, richtlijnen en procedures voor het initiëren, implementeren, onderhouden en verbeteren van information security management binnen een organisatie.

MUHAMMAD IMRAN Tariq, Haq, & Iqbal (2013) concluderen in hun onderzoek dat COBIT het wereldwijde aanvaarde IT Governance-framework is en dat COBIT Information Security domeinen heeft die voldoende zijn om Cloud organisaties te beveiligen.

Al-Hashimi, Al-Nidawi, Othman, Shakir, & Sulaiman (2019) geven in hun onderzoek aan dat de managementprocessen in het framework van National Institute of Standards and Technology (NIST) aan continue verbetering werken met behulp van een Plan, Do, Check, Act-cyclus om de informatiebeveiliging van organisaties effectief te beheren en te regelen.

In tabel 6 hieronder wordt weergegeven welke Information Security Frameworks in de verschillende artikelen gebruikt worden. In de kolom totaal is een opsomming gemaakt van de aantal keren dat de frameworks worden genoemd in verschillende artikelen. De meest voorkomende zijn respectievelijk CSA, NIST, ENISA, COBIT en ISO 27001 & 27000. De namen van de artikelen die in tabel 6 zijn opgenomen zijn terug te vinden in bijlage 1.

#	Framework	Rebollo et al. (2012)	Alnuem et al. (2015)	El-Hashimi et al. (2019)	Tariq (2012)	Tariq et al. (2013)	Negara et al. (2014)	Tariq et al. (2017)	Chen (2013)	Tariq (2012, July)	Totaal
1	European Union Agency for Network and Information Security (ENISA)	x		x	x		x			x	5
2	Cloud Cube Model	x		x							2
3	IT Control Objectives for Cloud Computing (ISACA)	x		x							2
4	Cloud Security Privacy	x		x							2
5	Security Guidance for Critical Areas of Focus in Cloud Computing (CSA)	x		x	x		x	x	x		6
6	Security and Control in the Cloud	x		x							2
7	ISO 27001 & 27000		x	x		x			x		4
8	National Institute of Standards and Technology (NIST)			x	x	x	x		x	x	6
9	Control Objectives for Information and related Technology (COBIT)				x	x	x			x	4

Tabel 6: Information Security Frameworks in Cloud omgevingen

Door 'Cloud' als zoekterm te gebruiken zijn er meer artikelen gevonden, echter geen enkel artikel geeft direct antwoord op deelvraag 2. Uit de gevonden resultaten kan niet geconcludeerd worden dat er één 'beste' Information Security Framework is dat gebruikt kan worden binnen een Cloud omgeving, dan wel binnen Continuous Deployment Pipelines. Dit omdat de verschillen van de aantallen te klein zijn.

Schinagl, Paans, & Schoon (2016) hebben in hun onderzoek meerdere standaarden voor Information Security & Privacy Protection met elkaar vergeleken zoals;

- United States National Institute of Standards and Technology (US NIST)[1]
- United States Federal Information Processing Standards (US FIPS)[2]
- United States Health Insurance Portability and Accountability Act (US HIPAA)[3]
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27001:2013)[4]
- Open Web Application Security Project (OWASP)[5]

[1] NIST is een wetenschappelijke instelling die onder de Amerikaanse federale overheid valt.
[2] De normen van FIPS worden ontwikkeld en gepubliceerd door de Amerikaanse federale overheid.
[3] HIPAA is de Amerikaanse wetgeving uit 1996 voor de gezondheidssector.
[4] ISO / IEC JTC 1 is een gezamenlijk technisch comité van de Internationale Organisatie voor Standaardisatie en de Internationale Elektrotechnische Commissie.
[5] Het OWASP is een open source-project rond computerbeveiliging.

- Control Objectives for Information and related Technology (COBIT) [6]
- Payment Card Industry Data Security Standard (PCI DSS) [7]
- Information Security Forum (ISF) Standard of Good Practice[8]

Ze hebben om de overlap en verschillen te bestuderen een eigen onderzoeksdatabase gecreëerd die de gedetailleerde measures van deze standaarden bevat. De conclusie van deze vergelijking is dat de hierboven genoemde standaarden vergelijkbare methoden gebruiken en bijna dezelfde gedetailleerde measures hanteren. Het onderzoek van Schinagl et al. (2016) is niet gefocust op Continuous Deployment Pipelines en geeft daarom niet een antwoord op deze specifieke deelvraag. Zij concluderen dat de measures van de verschillende standaarden in detail vaak hetzelfde zijn, wat wel interessant is voor dit onderzoek.

Om verder te gaan met het onderzoek is het nodig om één Information Security Framework te selecteren zodat er een basis overzicht gevormd kan worden van Information Security Measures/Controls dat verder uitgewerkt kan worden. Nader onderzoek toont aan dat de Information Security Forum (ISF) met ISF Standard of Good Practice for Information Security (2018) een zeer uitgebreid framework heeft ontwikkeld. Dit framework dekt de meeste frameworks af die hierboven genoemd zijn. De frameworks die ISF afdekt zijn;

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002; *nummer 7 volgens tabel 6*
- Control Objectives for Information and related Technology (COBIT) 5 for Information Security; *nummer 9 volgens tabel 6*
- Payment Card Industry Data Security Standard (PCI DSS) v3.2;
- the Center for Internet Security (CIS) Top 20 Critical Security Controls v.7;
- the National Institute of Standards and Technology (NIST) Cybersecurity Framework v.1.1.; *nummer 8 volgens tabel 6*

Doordat het ISF framework (2018) zeer uitgebreid is en de meeste security frameworks die in de literatuur zijn genoemd afdekt is er voor gekozen om dit framework verder aan te vullen in het empirische gedeelte van dit onderzoek.

2.3.3. Information Security Measures in Deployment Pipelines

In deze paragraaf wordt naar aanleiding van het literatuuronderzoek getracht antwoord te geven op deelvraag drie:

'Welke Information Security Measures kunnen gesteld worden aan een Continuous Deployment Pipeline?'

De termen measure(s) en control(s) wordt in de literatuur veel door elkaar gebruikt. Voor dit onderzoek is de definitie van een measure en control gehanteerd als beveiligingsmaatregel die genomen kan worden om kwetsbaarheden te voorkomen.

Ullah, Raft, Shahin, Zahedi, & Babar (2017) geven in hun onderzoek aan dat Continuous Deployment als een nieuwe praktijk is ontstaan in de software-industrie om softwareveranderingen continu en

[6] COBIT is een raamwerk gecreëerd door ISACA voor IT-beheer en IT-beheer.
[7] De PCI-standaard wordt beheerd door de Payment Card Industry Security Standards Council.
[8] The ISF is een leden organisatie.

automatisch in productie te implementeren. Continuous Deployment Pipeline (CDP) ondersteunt het uitvoeren van Continuous Deployments door de veranderingen in de repository te implementeren op productie. Aangezien de meeste CDP-componenten worden uitgevoerd in een omgeving met verschillende interfaces naar het internet, zijn deze componenten kwetsbaar voor verschillende soorten kwaadaardige aanvallen. In hun onderzoek hebben ze zich gericht op het ontwerpen van een veilige CDP door gebruik te maken van 'security tactics'. Ze benoemen in hun onderzoek drie key componenten die voor CDP van toepassing zijn. Voor deze key componenten zijn de Security Risks als volgt geïdentificeerd:

Component	Security Risks
Repository (GitHub)	Uncontrolled access
Main Server (AWS)	Poor authentication mechanism
	Uncontrolled access
CI server (Jenkins)	Starting build process with previously infected state
	Uncontrolled access

Tabel 7: Security Risks in Key Componenten van CDP volgens Ullah et.al. (2017)

Vervolgens geven Ullah et al. (2017) aan dat deze Security Risks gemitigeerd kunnen worden door de volgende vijf controls te implementeren;

1. Controlled Access to Repository
2. Enhanced Authentication Mechanism for Main Server
3. Controlled Access to Main Server
4. Clean CI Server VM Image
5. Controlled Access to CI Server

Hoewel dit artikel zich focust op 'Controlled access" en geen compleet beeld vormt, geeft het wel deels antwoord op de gestelde deelvraag.

Lang & Schreiner (2011) concluderen in hun onderzoek dat er een paar 'major gaps' zijn in de cloud gerelateerde security frameworks zoals NIST, ENISA, HIPAA etc. De gaps die interessant zijn voor deze deelvraag zijn:

- Er is te veel gefocust op identiteit en authenticatie en op nalatigheden op policy en autorisatie
- Security van de applicatie laag en de business proces laag wordt niet gedekt

De onderzoekers geven niet specifiek aan welke controls ontbreken en geven geen antwoord op de gestelde deelvraag.

Bass, Holz, Rimba, Tran, & Zhu (2015) hebben onderzoek gedaan naar de wijze van beveiliging van een deployment pipeline. In hun onderzoek hebben ze alleen gefocust op de integriteit van de deployment pipeline. Bass et al. (2015) geven in hun onderzoek aan dat ze kwesties zoals het lekken van gevoelige informatie naar een aanvaller negeren, tenzij dit lek ertoe leidt dat de aanvaller dergelijke inloggegevens kan verkrijgen. De onderzoekers geven geen duidelijk overzicht over welke requirements ze in de pipeline implementeren.

Koopman (2019) heeft in zijn afstudeeronderzoek een framework ontwikkeld om ontwikkelaars te helpen hun Continuous Delivery Pipeline veiliger te maken. Hij geeft aan dat hij dit framework heeft ontwikkeld omdat andere reeds bestaande frameworks te specifiek of te generiek zijn. Hij heeft

eerst Threats (bedreigingen) gedefiniëerd die gebaseerd zijn op het STRIDE model, vervolgens heeft hij in drie iteraties controls aan deze threats gekoppeld en gevalideerd met experts. De in totaal 80 gedefinieerde controls, die volgens Koopman (2019) gebaseerd zijn op het MITRE ATT&CK knowledge base en gezond verstand, kunnen gesteld worden aan een Continuous Delivery Pipeline. Met de gedefinieerde 80 controls heeft Koopman (2019) het meest complete antwoord gegeven op de gestelde deelvraag.

2.3.4. Automatisering van Information Security Measures

In deze paragraaf wordt naar aanleiding van het literatuuronderzoek getracht antwoord te geven op deelvraag vier:

'Welke Information Security Measures kunnen eenvoudig geautomatiseerd worden in een Continuous Deployment Pipeline?

Om deze deelvraag naar behoren te kunnen beantwoorden is eerst gezocht naar een definitie van automatisering binnen deze context. Montesino, Fenz, & Baluja (2012) hebben security automation als volgt gedefinieerd: "The automatic operation and monitoring of security controls by existing hard – and software security tools, reducing human intervention to a minimum. A security control can be automated if the operation of the control requires only machine-readable and – processable resources (for example, controls such as awareness and security training cannot be automated because they require the training of humans)" (Montesino et al., 2012).

Lang & Schreiner (2011) hebben verschillende security frameworks met elkaar vergeleken in hun onderzoek. In hun onderzoek concluderen ze dat "Security incident monitoring", "reporting" en "auditing" implementaties meer policy-driven geautomatiseerd moeten worden zodat real-time inzicht in security verbeterd kan worden. Lang & Schreiner (2011) geven niet aan wat of hoe dit geautomatiseerd kan worden.

Montesino et al. (2012) concluderen in hun onderzoek dat ongeveer 30 procent van de security controls die beschreven worden in internationale standaarden, zoals ISO 27001 en NIST SP 800-53 geautomatiseerd kunnen worden. Ze hebben in hun onderzoek deze security controls gegroepeerd in tien automatiseerbare security controls:

1. Asset inventory
2. Accountmanagement
3. Log Management
4. System Monitoring
5. Malware protection
6. Vulnerability scanning and patch management
7. Security configuration assessment and compliance checking
8. Information backup
9. Physical security
10. Incident management

Montesino et al. (2012) geven in hun onderzoek niet specifiek aan of deze controls ook in een Continuous Deployment Pipeline geautomatiseerd kunnen worden. Tevens geven ze de mate van eenvoudig van het automatiseren van de security controls ook niet aan. Hiermee is deze deelvraag deels beantwoord.

Rylander & Moberg (2018) hebben in een experiment onderzocht hoe key rotations in een Continuous Delivery Pipeline geautomatiseerd kunnen worden. De onderzoekers hebben

aangetoond dat key rotations volledig geautomatiseerd kunnen worden in de pipeline. Key management is volgens de onderzoekers nodig om ervoor te zorgen dat alleen geautoriseerde medewerkers toegang hebben tot de code en het proces kunnen doorlopen. Ze hebben in hun experiment de control niet getest, handmatig getest en geautomatiseerd getest. Hieronder wordt het tabel met de resultaten getoond.

	None	Manual	Automated
Average time	N/A	114.02 sec	1.60 sec
Minimum time	N/A	82.49 sec	1.32 sec
Maximum time	N/A	182.37 sec	2.74 sec
Added security	No	Yes	Yes
Cost in time	None	114.02 sec/key rotation	8 hours
Manual steps	None	20	None
Average downtime	None	5.62 sec	1.14 sec

Tabel 8: Vergelijking van de drie deployment pipelines volgens Rylander and Moberg (2018)

Dit onderzoek is alleen gefocust op automatisering van key management en geeft daarom geen volledig antwoord op de gestelde deelvraag.

2.3.5. Conclusie literatuuronderzoek

Doel van het literatuuronderzoek is om antwoord te krijgen op de centrale vraag: *Welke Information Security Measures kunnen geautomatiseerd worden binnen de Continuous Deployment Pipeline zodat Continuous Compliance bewerkstelligd kan worden?*

Om deze vraag te kunnen beantwoorden is er een aantal deelvragen opgesteld en in wetenschappelijke literatuur gezocht naar antwoorden.

De resultaten van de eerste deelvraag toont aan dat er in de wetenschappelijke literatuur geen bruikbare Continuous Compliance Framework bekend is dat toegepast kan worden binnen Continuous Deployment Pipelines (CDP). Echter hebben Derksen et al. (2018) in hun boek het model Agile Software Assurance Maturity Model (ASAMM) beschreven dat als basis gebruik zou kunnen worden voor een Continuous Compliance framework. Dit model beschrijft geen specifieke Information Security Measures die genomen kunnen worden binnen een CDP.

De resultaten van de tweede deelvraag tonen aan dat er niet één lijn te trekken is met de security frameworks die gebruikt kunnen worden binnen CDP's. Tevens heeft een vergelijkingsonderzoek van Schinagl et al. (2016) tussen verschillende standaarden aangetoond dat op measures niveau tussen de standaarden weinig verschillen zijn gevonden. Om verder te gaan met het onderzoek is gekozen voor het framework Information Security Forum (ISF) met ISF Standard of Good Practice for Information Security (2018). Dit omdat dit framework zeer uitgebreid is en de meeste security frameworks die in de literatuur zijn genoemd afdekt.

De derde deelvraag is het best beantwoord door het framework van Koopman (2019). In dit afstudeeronderzoek is een lijst met 80 gedefinieerde controls gedefinieerd die gesteld kunnen worden aan een CDP.

De resultaten van de vierde deelvraag tonen Montesino et al. (2012) aan dat 30% van de security controls van standaarden zoals NIST en ISO 27001 te automatiseren zijn echter is in dit onderzoek geen relatie gelegd naar een CDP. In een ander onderzoek van Rylander & Moberg (2018) wordt aangetoond dat één control volledig te automatiseren is.

De uitkomst van het literatuuronderzoek en antwoord op de centrale vraag is als volgt:

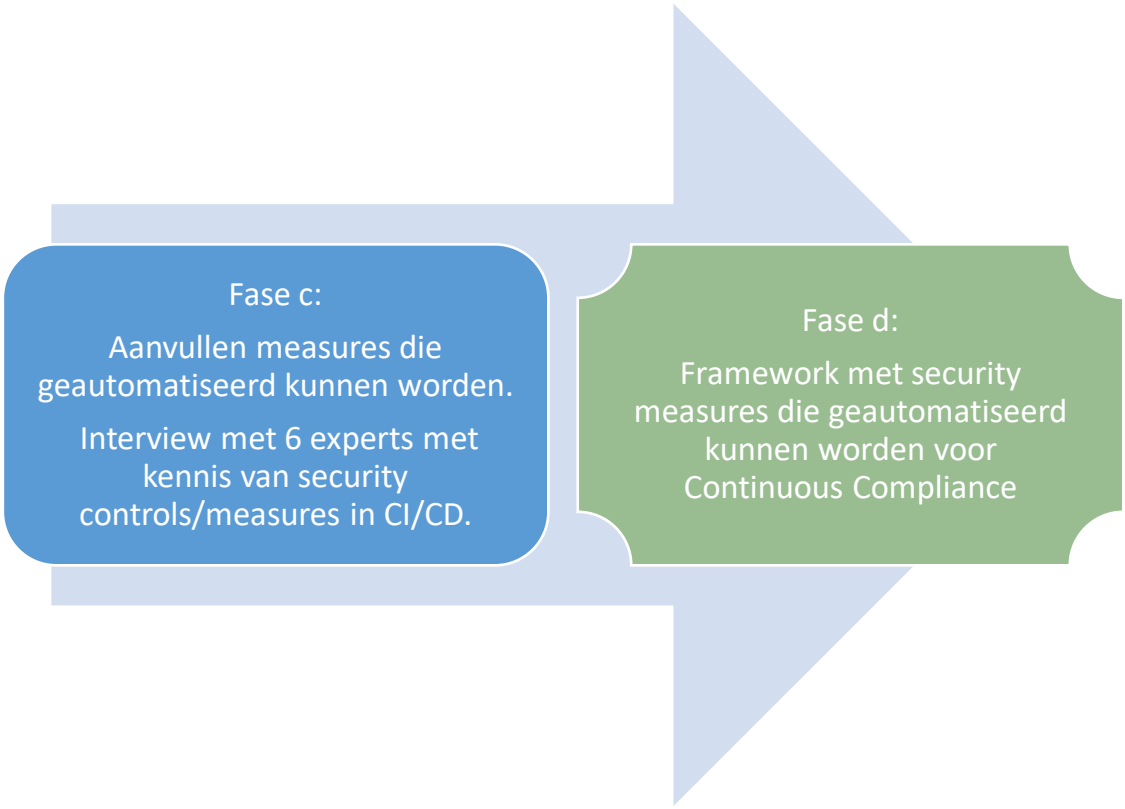
Uit het literatuuronderzoek is gebleken dat er geen éénduidige manier en/of overzicht is om Information Security Measures geautomatiseerd te integreren in een Continuous Deployment Pipeline.

In het algemeen kan naar aanleiding van de resultaten geconcludeerd worden dat onderzoeken in de wetenschappelijke literatuur erg schaars zijn over dit onderwerp. Dit gezegd hebbende, is de eindconclusie van het literatuuronderzoek als volgt:

Er is een lacune in de wetenschappelijke literatuur over Continuous Compliance, Information Security Measures (Controls) die geautomatiseerd kunnen worden in een Continuous Deployment Pipeline. Empirisch onderzoek zou deze lacune in de literatuur kunnen opvullen.

2.4. Doel van het vervolgonderzoek

Doelstelling van het empirisch onderzoek luidt als volgt: Het opleveren van een framework van Information Security Measures die geautomatiseerd kunnen worden in een Continuous Deployment Pipeline.



Figuur 5: Doel empirisch onderzoek

In fase c wordt op basis van het ISF framework een lijst met Information Security Measures getoetst met experts of deze geautomatiseerd kunnen worden in een Continuous Deployment Pipeline.

Vervolgens wordt in fase d op basis van de resultaten uit de interviews met de zes experts de lijst met Information Security Measures verwerkt. Met deze aanvullingen ontstaat een aangevuld framework met Information Security Measures die geautomatiseerd kunnen worden in Continuous Deployment Pipeline.

Aanvullend aan de vraag of de Information Security Measures geautomatiseerd kunnen worden zal ook gevraagd worden aan de experts hoe eenvoudig het is om de measures te automatiseren en hoeveel tijd het ongeveer kost om de measures handmatig en geautomatiseerd te testen.
Deze aanvullende informatie kan een bijdrage leveren aan ontwikkelaars om de volgorde van implementatie te bepalen van de measures die geautomatiseerd kunnen worden.

3. Methodologie

In dit hoofdstuk is de methode voor het empirisch onderzoek beschreven.

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n)

Het uiteindelijke doel van het empirisch onderzoek is het opleveren van een lijst van Information Security Measures die geautomatiseerd kunnen worden zodat een Continuous Compliance Framework bewerkstelligd kan worden.

Om dit doel te kunnen behalen is het nodig om de samengestelde lijst met Information Security Measures die geautomatiseerd kunnen worden te valideren bij experts en per measure te laten beoordelen op de mate van complexiteit om het te automatiseren.

Uit de resultaten van het literatuuronderzoek is gebleken dat de antwoorden op de deelvragen niet eenvoudig te vinden zijn in de wetenschappelijk literatuur. Om deze lacune aan te vullen zullen tijdens het empirisch onderzoek de experts geraadpleegd worden om antwoorden op de gestelde deelvragen te kunnen krijgen. Deze deelvragen zullen hetzelfde zijn als in het literatuuronderzoek.

3.1.1. Deductief of Inductief?

Een belangrijke vraag bij het bepalen van de onderzoeksstrategie die volgens Saunders, Lewis, & Thornhill (2015) beantwoord moet worden, is de vraag of het onderzoek gebaseerd is op de deductieve of inductieve methode. De deductieve methode wordt gebruikt bij een bestaande theorie of een bestaand model om een hypothese te formuleren en een onderzoeksmethode te ontwerpen om deze hypothese te toetsen. Bij de inductieve methode wordt data verzameld en een theorie of model ontwikkeld. Dit onderzoek zal meer exploratief van aard zijn en om deze reden is de inductieve benaderingsmethode het meest geschikt.

3.1.2. Kwalitatief of kwantitatief?

Om tot de antwoorden op de deelvragen te komen is een kwalitatieve benadering gewenst, omdat de deelvragen verkennend zijn. Er wordt in dit onderzoek op een systematische manier gegevens verzameld. Deze gegevens worden geanalyseerd en aangevuld door een zes experts.

3.1.3. Welke onderzoeksmethoden?

Saunders et al. (2015) beschrijft de volgende onderzoeksmethode die toegepast kan worden om de deelvragen te beantwoorden.

Het surveyonderzoek;

Volgens Saunders et al. (2015) wordt een surveyonderzoek veel gebruikt om op een zeer economische wijze een grote hoeveelheid data uit een omvangrijke populatie te verzamelen. De kenmerken waaraan je een survey kan herkennen zijn als volgt:

- Een ruim domein
- Arbeidsintensieve data-generatie
- Meer breedte dan diepte
- Een selecte steekproef
- Kwantitatieve data en analyse

Volgens Saunders et al. (2015) is een aanpak met meerdere methoden nuttig als hierdoor de onderzoeksvragen beter beantwoord kunnen worden. Voor dit onderzoek is gekozen voor de

gemengde methode ('mixed methods'), waarbij gebruikt wordt gemaakt van het surveyonderzoek en de Design Science Research methode. In de volgende paragraaf wordt de keuze voor deze methode nader toegelicht.

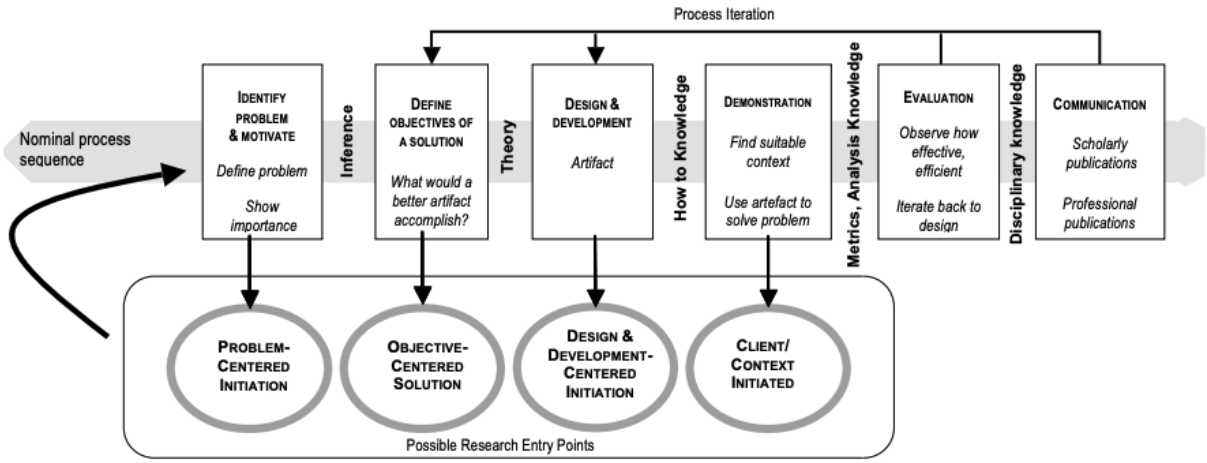
3.1.4. Ontwerpgericht onderzoek

In dit onderzoek is de Design Science Research (DSR) methode gekozen. Het voordeel van een DSR aanpak is dat het vooral een "probleem oplossend paradigma" is dat gericht is op het "creëren en evalueren van innovatieve IT-artefacten (Hevner, March, Park, & Ram, 2004).

Het doel van dit onderzoek is om het probleem met het handmatig verzamelen van bewijsmateriaal in spreadsheets op te lossen door de Information Security Measures te automatiseren in een Continuous Deployment Pipeline. Door te onderzoeken welke Information Security Measures geautomatiseerd kunnen worden kan het Continuous Compliance Framework bewerkstelligd worden dat als artefact zal fungeren. Het toepassen van design science research past om deze reden bij het doel van dit onderzoek.

Volgens Peffers, Tuunanen, Rothenberger, & Chatterjee (2007) bestaat een design science research proces uit zes stappen:

1. Probleem identificatie & motivatie
2. Doelstellingen van een oplossing
3. Ontwerp & Ontwikkeling
4. Demonstratie
5. Evaluatie
6. Communicatie



Figuur 6: DSRM proces model volgens Peffers et al., (2007)

Afhankelijk van het doel van het onderzoek kan het 'Entry Point' worden bepaald. Het voorgaande literatuuronderzoek heeft de eerste twee processtappen en een gedeelte van stap drie doorlopen. Stap drie is in het empirisch onderzoek verder onderzocht.

De resultaten uit het literatuuronderzoek (fase a, figuur 2) zijn geschikt om het framework vooraf (fase b, figuur 2) te structureren, zodat deze verder aangevuld kan worden met kwalitatieve data dat verzameld zal worden uit de interviews met de experts (fase c, figuur 2).

Onderstaand een tabel hoe de faseringen van de Design Science Research Methode Peffers et al. (2007) en het onderzoeksmodel van Verschuren & Doorewaard (2007) dat in paragraaf 1.6 is beschreven overeenkomen. In de laatste kolom staat aangegeven in welk hoofdstuk of paragraaf de faseringen zijn uitgewerkt.

(Peffers et al., 2007)	(Verschuren & Doorewaard, 2007)	Behandeld in Hoofdstuk/Paragraaf
Probleem identificatie & motivatie	Fase a	H1.1 t/m H1.4
Doelstellingen van een oplossing	Fase a	H1.5
Ontwerp & Ontwikkeling	Fase b, c & d	H2, H3 & H4
Demonstratie	n.v.t.	n.v.t.
Evaluatie	n.v.t.	n.v.t.
Communicatie	n.v.t.	n.v.t.

Tabel 9: Peffers et al. (2007) versus Verschuren & Doorewaard (2007)

Het ontwerp is niet gevalideerd in dit onderzoek. Daarom worden alleen de eerste drie stappen, probleem identificatie en motivatie, doelstellingen van een oplossing (H1) en ontwerp & ontwikkeling (H2, H3 en H4) verder uitgewerkt.

3.2. Technisch ontwerp: uitwerking van de methode

In deze paragraaf wordt beschreven op welke manier het onderzoek wordt aangepakt en waarom de genomen beslissingen gepast zijn. Per deelvraag zal er uitleg gegeven worden welke gegevens nodig zijn om de deelvraag te kunnen beantwoorden. Bij welke bronnen deze gegevens gehaald worden en hoe ze verzameld zullen worden.

Design Science Research is gericht om een probleem op te lossen, echter wordt niet beschreven hoe de gegevens verzameld moeten worden om een model te ontwikkelen. In dit onderzoek is gekozen om gegevens te verzamelen via semi-gestructureerd interviews die gehouden zullen worden met experts. Tevens zal aan de experts gevraagd worden om een vragenlijst voorgaand aan het interview in te vullen.

Om de experts op een systematische wijze te selecteren, zodat er geen belangrijke details uit het oog worden verloren, is gezocht naar literatuur die dit ondersteund.

Okoli & Pawlowski (2004) hebben een proces ontwikkeld voor het selecteren van gekwalificeerde experts. Om dit proces te volgen moet eerst een Knowledge Resource Nomination Worksheet (KRNW) voorbereid worden. Het doel van de KRNW is om de experts te categoriseren voordat ze worden geïdentificeerd, om te voorkomen dat een belangrijke klasse experts over het hoofd wordt gezien.

Het proces om experts te selecteren bestaat volgens Okoli & Pawlowski (2004) uit vijf stappen:

Stap 1: Voorbereiden KRNW	• Identificeren van relevante vakgebieden, vaardigheden en gerelateerde literatuur
Stap 2: De KRNW vullen met namen	• Namen verzamelen van individuen die voldoen aan de relevante vakgebieden en vaardigheden
Stap 3: Benoemen van andere experts	• Contact opnemen met de experts • De experts vragen om andere experts aan te dragen
Stap 4: Categoriseren experts	• Categoriseren van alle experts
Stap 5: Uitnodigen experts	• Uitnodigen van alle experts om deel te nemen aan het onderzoek

Tabel 10: Procedure om experts te selecteren volgens Okoli & Pawlowski (2004)

In de volgende paragrafen zal per deelvraag de onderzoekmethode toegelicht worden, hoe de gegevens verzameld zullen worden en aan welke eisen de experts aan moeten voldoen.

Ontwerp & Ontwikkeling

In het DSRM proces is het ontwikkelen van een IT-artefact stap drie. In het onderzoeksmodel is dit fase b & c. Fase b is al in het literatuuronderzoek afgerond, in fase c is het IT-artefact verder aangevuld samen met expert door semi-gestructureerde interviews te houden.

Semi-gestructureerd interview

Er is gekozen voor een semi-gestructureerd interview, omdat de onderzoeker hiermee deels de vrijheid heeft om te improviseren naar aanleiding van de gegeven antwoorden. Er zal een lijst met thema's en vragen behandeld worden tijdens de interviews. De volgorde van de vragen kan ook veranderen naargelang het verloop van het gesprek. Anderzijds kunnen er extra vragen nodig zijn om de onderzoeksvragen en doelstellingen verder te onderzoeken (Saunders et al., 2015).

De zes experts die in deze fase geïnterviewd worden, dienen te voldoen aan de volgende criteria:

- Kennis hebben van Continuous Delivery
- Kennis en ervaring hebben met Security Measures/Controls in een CI/CD omgeving
- Kennis hebben van Compliance processen
- Kennis hebben van het ISF framework
- Minimaal 5 jaar werkervaring met Continuous Delivery
- Volgt nieuwe ontwikkelingen rondom Continuous Delivery
- Tenminste HBO werk- en denkniveau

Voorafgaand aan het interview zijn de experts voorzien van de volgende stukken:

- Een introductie e-mail over het doel van het onderzoek
- Uitleg over wat de experts moeten voorbereiden
- Lijst met definitie van de gebruikte termen
- Lijst met de 131 Information Security Measures dat gebaseerd is op ISF Standard of Good Practice for Information Security (2018) waarvan bepaald moet worden of deze te automatiseren zijn in een Deployment Pipeline

Bovenstaande punten en de deelvragen die in het semi-gestructureerd interview gevraagd zijn aan de experts zijn opgenomen in het interview protocol in bijlage 3.

In tabel 11 is opgenomen welke interviewvragen zijn gesteld en welke kennis de antwoorden op deze vragen oplevert.

#	Interviewvraag	Opgeleverde kennis
1	Wat is jouw definitie van Continuous Compliance (CC)? - Wat is een bruikbaar framework voor CC? - Waar zal een CC Framework aan bijdragen?	Er is in de literatuur geen bruikbare framework van CC en geen definitie van CC gevonden, door de antwoorden van de experts te destilleren kan een definitie geformuleerd worden van CC. Indien de experts een bruikbaar CC framework al kennen dan kan deze framework als basis gebruikt worden om vervolgonderzoek verder vorm te geven en de literatuur te verrijken. Tevens geeft dit antwoord inzicht of een CC framework volgens de experts een nuttige bijdrage zal leveren.
2	Welke Information Security Frameworks worden veelal gebruikt binnen een Continuous Deployment Pipeline? - Wordt er binnen jouw bedrijf een bepaalde framework gebruikt in de Deployment Pipelines?	Indien bepaalde Security Frameworks al toegepast worden binnen Deployment Pipelines, zal dit antwoord inzicht geven of binnen de organisatie van de experts al een bepaalde keuze gemaakt is voor een framework, deze frameworks zouden dan als uitgangspunt genomen kunnen worden in eventuele vervolgonderzoek.
3	Welke Information Security Measures kunnen gesteld worden aan een Continuous Deployment Pipeline? - Wat voor soort Measures kunnen in een Pipeline geautomatiseerd worden en waarom?	Dit antwoord zal inzicht geven in wat voor soort Security Measures binnen Deployment Pipelines gesteld kunnen worden. Op basis van de gegeven antwoorden kan eenvoudiger gecategoriseerd worden welke 131 Security Measures van ISF relevant zijn voor Deployment Pipelines.
4	Welke Information Security Measures kunnen eenvoudig geautomatiseerd worden in een Continuous Deployment Pipeline? - Welke criteria heb je gehanteerd om te kunnen bepalen of de Information Security Measures eenvoudig te automatiseren zijn? - Zijn er binnen jouw bedrijf Information Security Measures geautomatiseerd in een Pipeline? - Vind je dat waar mogelijk alle Information Security Measures geautomatiseerd moeten worden en waarom? - Vind je het ISF framework een goed vertrekpunt om de Information Security Measures te automatiseren en waarom?	De experts hebben vooraf aan het interview een vragenlijst ingevuld met 131 Information Security Measures waarbij ze per measure de mate van eenvoudigheid om te automatiseren hebben aangegeven. De antwoorden op deze deelvraag geven inzicht in hoe ze de lijst hebben ingevuld, of ze het de moeite waard vinden om deze Measures te automatiseren en of ze het ISF framework wel een geschikte vertrekpunt vinden om te automatiseren binnen Deployment Pipelines.

Tabel 11: Interviewvragen en opgeleverde kennis

Op basis van de gegeven antwoorden is het IT-artefact verder ontworpen en ontwikkeld waarmee een aangevuld framework is ontstaan. De resultaten van het aangevuld framework worden niet gevalideerd in dit onderzoek.

Proefvoorbereiding en proefinterview

Om tot een goede inschatting te kunnen komen van de gevraagde tijdsbesteding en de duidelijkheid van de onderzoeksvragen te toetsen is een proefinterview gehouden met een controle respondent die bekend is met de begrippen Continuous Compliance, Deployment Pipelines en Information Security Measures. Dit om de vraagstelling te testen en de volledigheid van de vragen te beoordelen. Tevens is de controle respondent gevraagd om een spreadsheet met de 131 Information Security Measures in te vullen om deelvraag vier te kunnen beantwoorden. Vooraf aan het interview heeft de controle respondent aangegeven dat het invullen van de spreadsheet twee uur heeft gekost. Het proefinterview met de controle respondent heeft ongeveer 20 minuten geduurd. Naar aanleiding van het proefinterview en de gegeven feedback is het interviewprotocol, de gehanteerde definities en een aantal interviewvragen aangescherpt.

Selectie participanten

De participanten zijn geselecteerd op basis van het expert selectie proces (Okoli & Pawlowski, 2004). Er zijn meerdere experts benaderd en zes daarvan zijn geïnterviewd.

De experts zijn deels telefonisch en deels persoonlijk benaderd om te vragen of ze geïnteresseerd waren om deel te nemen aan dit onderzoek. Bij een positief antwoord is een uitnodigingsemail gestuurd met uitleg over hoe de expert zich kon voorbereiden op het interview.

De experts zijn gecategoriseerd in twee aandachtsgebieden. Categorie A heeft diepgaande technische kennis en kan zelf code programmeren, categorie B heeft theoretische technische kennis en heeft geen ervaring met code ontwikkeling. Alle experts voldoen aan de gestelde expertcriteria. De experts hebben allemaal verschillende rollen en werken binnen verschillende Business Units in dezelfde financiële instelling.

Participant	Categorie	Technische kennis
1	A	Diepgaande technische kennis & ervaring met code programmeren
2	A	Diepgaande technische kennis & ervaring met code programmeren
3	A	Diepgaande technische kennis & ervaring met code programmeren
4	B	Theoretische technische kennis & geen ervaring met code programmeren
5	B	Theoretische technische kennis & geen ervaring met code programmeren
6	B	Theoretische technische kennis & geen ervaring met code programmeren

Tabel 12: Categorisering experts

Voorbereiding participanten

De zes experts hebben een e-mail (bijlage 2) met een introductie over het doel van het onderzoek gekregen. Tevens zijn de gehanteerde definities beschreven en is uitgelegd wat de experts vooraf aan het interview moeten voorbereiden.

Als bijlage is de spreadsheet met de 131 Information Security Measures dat gebaseerd is op ISF Standard of Good Practice for Information Security (2018) meegestuurd met het verzoek deze lijst in te vullen. De experts konden per measure met een vijfpunts-Likertschaal aangeven wat de moeilijkheidsgraad is om de measure te automatiseren in een deployment pipeline. Tevens is aanvullend gevraagd hoeveel tijd het zou kosten om de measure handmatig te testen.

De volgende uitleg is gegeven bij de twee kolommen die ingevuld moesten worden:

Kolom L: Automatability? Hier kun je aangeven wat je eigen inschatting is op basis van je expertise hoe makkelijk of moeilijk het is om het desbetreffende Topic te automatiseren in een Continuous Deployment Pipeline.

Kolom M: Manual time? Hier kun je aangeven hoeveel tijd het ongeveer zou kosten als je bestaande bewijsmateriaal handmatig zou gaan verzamelen om aan te tonen dat je aan het desbetreffende Topic voldoet. Ervan uitgaande dat je voldoet aan het topic en dat het bewijsmateriaal bestaat maar nog niet eerder is verzameld.

3.3. Gegevensanalyse

De gegevens die verkregen zijn uit de semi-gestructureerd interviews zijn kwalitatief van aard. Tijdens deze interviews is een logboek bijgehouden en audio opnames gemaakt. Achteraf zijn de audio opnames beluistert en zijn er transcripten gemaakt die ter review gestuurd zijn naar de participanten.

De gegevens die verkregen zijn uit de ingevulde vragenlijsten zijn kwantitatief van aard. Volgens Saunders et al. (2015) zal de verkregen ruwe data niet altijd bruikbare data opleveren, omdat respondenten halverwege de vragenlijst kunnen stoppen of de vragenlijst kunnen afraffelen. Om de verkregen ruwe data betekenis te geven is dit verwerkt in informatie door de ruwe data om te zetten naar een databestand voor het uitvoeren van statistische analyses.

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

In deze paragraaf zal beargumenteerd worden waarom het onderzoek op een wetenschappelijk verantwoorde manier is opgezet.

Validiteit

Saunders et al. (2015)definieert validiteit als volgt;

1. De mate waarin methoden voor het verzamelen van gegevens nauwkeurig meten wat ze zouden moeten meten
2. De mate waarin onderzoeksresultaten werkelijk betrekking hebben op datgene waar ze betrekking op zouden moeten hebben.

Om de validiteit van dit onderzoek te bevorderen zijn de volgende maatregelen genomen:

Voorafgaand aan de semi-gestructureerde interviews krijgen de experts een uitnodiging met daarin uitleg over de thema's en definities over de gehanteerde termen zoals wat wordt verstaan onder "automatisering". Het doel van het interview wordt ook vooraf bekend gemaakt zodat de experts er alvast over kunnen nadenken. De semi-gestructureerde interviews vinden plaats in afgesloten vergaderkamers, zodat externe factoren minimaal storen.

In de gestructureerde interviews wordt vooraf aan de oorspronkelijke enquête definities gegeven van de gehanteerde termen en tevens uitleg over de thema's.

Betrouwbaarheid

Door gebrek aan standaardisatie bij de semi-gestructureerde interviews kan volgens Saunders et al. (2015) bezorgdheid ontstaan over de betrouwbaarheid.

De volgende maatregelen zijn genomen om de betrouwbaarheid van de semi-gestructureerde interviews te verhogen;

- De vragen die gesteld worden aan de geïnterviewde experts zijn zoveel mogelijk open en kort

- De definities van termen zijn vooraf gedeeld met de experts waardoor discussie over terminologie zoveel mogelijk gemitigeerd wordt
- De experts krijgen vooraf achtergrondinformatie waardoor ze weten wat hen te verwachten staat tijdens het interview
- Aan het eind van het interview zal de onderzoeker aan de hand van de gemaakte audio opname een transcript van het interview, zodat de experts hier feedback op kunnen geven
- De interviews zullen, met toestemming vooraf, opgenomen worden en binnen enkele dagen uitgewerkt in het transcript zodat de experts kunnen controleren of de uitwerking klopt
- De experts zal gevraagd worden om binnen twee weken te reageren op het transcript
- Vooraf zal een proefinterview gehouden worden met een collega die kennis heeft van dit domein om vast te stellen of de vragen begrijpelijk zijn, de tijdsduur niet te lang is, en of er antwoorden gegeven worden waarmee de onderzoeksvragen beantwoorden kunnen worden

Repliceerbaarheid

Repliceerbaarheid karakteriseert in hoeverre onderzoeksprocedures herhaalbaar zijn. Het principe stelt dat de procedures waarmee onderzoeksoutputs worden gecreëerd zodanig moeten worden uitgevoerd en gedocumenteerd dat anderen buiten het onderzoeksteam de procedures onafhankelijk kunnen herhalen en vergelijkbare, zo niet identieke resultaten kunnen verkrijgen (Recker, 2013).

Binnen dit onderzoek zijn de volgende maatregelen genomen om de repliceerbaarheid te verhogen;

- Zoekkaders en zoektermen zijn per deelvraag gedocumenteerd
- Gevonden resultaten tijdens het literatuuronderzoek zijn systematisch bijgehouden met URL naar de bron
- De vragenlijsten die tijdens de interviews worden gehouden zijn opgenomen als bijlage
- De bevindingen uit het empirisch onderzoek zijn zorgvuldig en zeer gedetailleerd gedocumenteerd

Controleerbaarheid

Volgens Saunders et al. (2015) valt en staat de kwaliteit van het onderzoek met de transparantie. Met transparantie wordt controleerbaarheid bedoeld; de mate waarin beoordeeld kan worden wat er tijdens een onderzoek is gedaan, hoe dat is uitgevoerd en welke gegevens dat heeft opgeleverd.

Binnen dit onderzoek zijn de volgende maatregelen genomen om de controleerbaarheid te verhogen;

- Onderzoeksmethode is in detail gerapporteerd
- De beperkingen van het onderzoek zijn uitvoerig beschreven
- De gegevens die geleid hebben tot resultaten en conclusies zijn beschikbaar gesteld zoals transcripten van de interviews
- Ingevulde gegevens van enquêtes zijn geanonimiseerd beschikbaar
- Kort cyclische onderzoeksbegeleiding met promotor

Ethische aspecten

Volgens Saunders et al. (2015) worden persoonsdata gedefinieerd als informatie die verband houdt met bepaalde geïdentificeerde of te identificeren personen. Wanneer je dit soort data verwerkt en beheert, zal je werk vallen onder de bepalingen van de wetgeving voor de bescherming van data van het land waarin je woont. Binnen dit onderzoek wordt niet veel met persoonsdata gewerkt. Enige persoonsdata zijn de namen en functies van de experts. Vanuit ethisch oogpunt zal bij verwerking van de interviews de namen van de experts geanonimiseerd worden.

In tabel 13 volgt een overzicht van ethische aspecten en de genomen maatregelen.

Aspect	Gevolg/Maatregel
Claim op tijd en resources	In de uitnodigingen voor de interviews wordt op voorhand een realistische inschatting gegeven van de tijd die gevraagd wordt van de respondent voor het voorbereiden van het interview, het interview zelf en de validatie van het interviewverslag achteraf.
Gevoeligheid onderwerp	In de gesprekken wordt duidelijk gemaakt dat het niet gaat om de organisatie af te rekenen op prestaties, maar te kijken naar mogelijkheden voor reductie van uitstoot en bijbehorende besparingen die gerealiseerd kunnen worden
Vertrouwelijkheid en anonimiteit	In dit onderzoek wordt de anonimiteit van de respondenten gewaarborgd door enkel hun initialen te gebruiken in databastanden en verslagen. Verder worden de interviewverslagen niet openbaar gepubliceerd maar opgeslagen bij de OU. Citaten die relevant zijn voor dit onderzoek worden in het kader van de transparantie in het verslag zelf opgenomen.Daarnaast worden er alleen opnames gemaakt van de interviews als de respondent daar expliciet toestemming voor heeft gegeven. De opnames worden niet gedeeld met derden.
Integriteit en objectiviteit van de onderzoeker	De onderzoeker is werkzaam binnen de organisatie waar het onderzoek wordt uitgevoerd. Bij de selectie van de respondenten moeten respondenten die een directe hiërarchische relatie hebben met de onderzoeker zoveel mogelijk worden uitgesloten van deelname. Indien er tijdens het onderzoek sprake is van een hiërarchische relatie dan zal dit worden aangemerkt. Verder kan de onderzoeker over voorkennis beschikken met betrekking tot de organisatie, het proces en/of personen.
Vrijwillige deelname en recht op terugtrekken	De deelname aan dit onderzoek is vrijwillig en staat er geen (geldelijke) beloning tegenover. Dit zal bij de uitnodigingen expliciet vermeld worden. Eveneens mag een ‘kandidaat’ respondent weigeren zonder dat er om een verdere toelichting wordt gevraagd. Indien dit gebeurt dan wordt een respondent gezocht met een gelijke functie/rol.
Informeren van respondenten	De respondent wordt vooraf uitgebreid geïnformeerd over het doel van het onderzoek. Hierbij worden de concepten uit het theoretisch kader toegelicht en wordt de checklist vooraf verstrekt.

Tabel 13: Ethische aspecten (Saunders, 2016)

4. Resultaten

In dit hoofdstuk is ten eerste de uitvoering van het empirisch onderzoek beschreven en ten tweede zijn de opgeleverde resultaten beschreven.

4.1. Uitvoering onderzoek

Uitvoering interviews

De interviews met de zes experts zijn één op één gehouden in een afgesloten vergaderruimte om afleiding door omgevingsfactoren te minimaliseren. Er zijn audio opnames gemaakt die vervolgens zijn getranscribeerd. Tijdens het terugluisteren en transcriberen van de opnames heeft de onderzoeker af en toe moeite gehad met het verstaan van sommige experts. Dit kwam voornamelijk omdat sommige experts heel snel praatten. Om deze reden zijn de transcripten ter review naar de participanten opgestuurd om er zeker van te zijn dat alle gegeven antwoorden wel goed zijn overgenomen. De feedback en eventuele aanvullingen op de transcripten zijn verwerkt voordat deze geanalyseerd zijn. De interviews zijn in het Nederlands gehouden en hebben gemiddeld, exclusief de introductie en toelichting op het onderzoek, 20 minuten in beslag genomen. De transcripten kunnen opgevraagd worden bij de Open Universiteit.

Tijdens het invullen hebben twee experts de onderzoeker gebeld met de vraag hoe ze kolom M, Manual time? moesten interpreteren. De uitleg in de e-mail over “Manual time” bleek niet duidelijk genoeg te zijn. Hier is telefonisch nader uitleg over gegeven.

Participant	Datum interview	Duur interview (min)
1	17/10/2019	21:40
2	22/10/2019	20:08
3	22/10/2019	14:16
4	24/10/2019	20:26
5	24/10/2019	23:07
6	28/10/2019	20:04

Tabel 14: Overzicht expertinterviews

Verwerking resultaten

De transcripten van de interviews zijn middels de grounded theory benadering van Strauss & Corbin (2008) gecodeerd en geanalyseerd. In eerste instantie is de data opgedeeld, gelabeld en gecategoriseerd middels open coderen. Vervolgens is er gezocht naar verbanden tussen de verschillende categorieën middels axiaal coderen. Als laatste stap zijn door middel van selectief coderen de concepten uitgewerkt in de resultaten binnen dit hoofdstuk. In een sessie op datum 21-02-2020 zijn met scriptiebegeleider Prof. dr. Yuri Bobbert aan de hand van de theorieën de belangrijke bevindingen uit de gehouden interviews gedefinieerd. De transcripten worden als **vertrouwelijk** behandeld en worden daarom niet als bijlage toegevoegd. De transcripten kunnen wel opgevraagd worden bij Open Universiteit.

4.2. Continuous Compliance Framework

In het voorgaande literatuuronderzoek is geen duidelijke definitie van Continuous Compliance in de peer reviewed artikelen gevonden. Om deze reden is getracht om een definitie van het begrip Continuous Compliance te formuleren op basis van de resultaten uit de interviews die zijn gehouden in het kader van dit onderzoek. Vervolgens is deze geformuleerde definitie verstuurd naar alle zes respondenten, waarvan vier bevestigend en twee niet hebben gereageerd.

Definitie Continuous Compliance:

Middels door interne en/of externe regelgeving vooraf gedefinieerde Information Security en Privacy policies en standaarden de nodige maatregelen (measures) inrichten binnen deployment pipelines om de daarbij behorende doelstellingen via controlemaatregelen effectief en continu te realiseren, te administreren en over te rapporteren naar relevante stakeholders.

Uit de interviews kwam naar voren dat er niet direct een bestaand Continuous Compliance framework voor handen is of niet bekend bij de respondenten. Respondent vijf geeft aan dat het moeilijk is omdat een framework vaak op hoger niveau wordt opgesteld en dat met Continuous Compliance vaak rule based zaken wordt geïmplementeerd.

Volgens de respondenten kan een Continuous Compliance framework wel bijdrage leveren aan het beheerst naar productie gaan. Het kan scoping en kader geven waar je aan moet voldoen, dit maakt het automatiseren van bewijsmateriaal makkelijker. Een framework geeft een richting en je kunt keuzes maken wat je eruit gebruikt. Respondent twee geeft aan dat je met een erkend framework kan voorkomen dat bedrijven het wiel opnieuw moeten uitvinden. Respondent drie geeft aan dat een Continuous Compliance framework ook zal bijdragen aan geautomatiseerd evidencen, hierdoor kun je sneller aantonen dat je in control bent waarmee je een tijdsbesparing oplevert. Respondent zes geeft aan dat een framework zal bijdragen aan een kostenbesparing doordat een framework kan zorgen voor efficiëntie en effectiviteit.

4.3. Information Security Frameworks

Tijdens de interviews is geen duidelijk antwoord gekomen op de vraag welke Information Security Frameworks binnen Deployment Pipelines gebruikt worden. Wel worden er allerlei varianten genoemd zoals OWASP en SANS top 20 of tools zoals Nessus en Fortify on Demand, maar deze kennen geen specifieke Continuous Deployment Pipeline framework. Ook noemen de respondenten specifieke fabrikant configuratie richtlijnen. Sommige respondenten hebben het ISF framework als voorkeur, omdat deze vrij compleet is. Andere respondenten hebben het CIS of NIST framework als voorkeur, omdat deze frameworks specifieker en technischer van aard zijn.

4.4. Information Security Measures in Continuous Deployment Pipelines

Op de vraag wat voor soort measures in een pipeline geautomatiseerd kunnen worden is aan de hand van de gegeven antwoorden sterk naar voren gekomen dat technische measures, zoals bijvoorbeeld secure code scanning en vulnerability scanning vrij makkelijk te automatiseren zijn.

Daarnaast is meerdere keren het automatiseren van de procesmatige checks in de pipeline genoemd, zoals het vierogen principe of approvals binnen de pipeline. De procesmatige checks zijn moeilijker te automatiseren, maar niet onmogelijk volgens een aantal respondenten. Wat wel moeilijk wordt om te automatiseren binnen de deployment pipelines zijn de meer proces georiënteerde zaken die bijvoorbeeld over governance controls gaan. De antwoorden die de respondenten hebben gegeven zijn veelal uitlopend wat mogelijk verklaard kan worden doordat het ISF framework ook hoog over is.

4.5. Automatisering van Information Security Measures

Om de vraag over welke Information Security Measures eenvoudig geautomatiseerd kunnen worden in een Continuous Deployment Pipeline te kunnen beantwoorden, was enige voorbereiding van de respondenten voorgaand aan de interviews nodig. De respondenten hebben een spreadsheetlijst ingevuld met de 131 Information Security Measures die gebaseerd zijn op ISF Standard of Good Practice for Information Security (2018).

De respondenten konden per measure met een vijfpunts-Likertschaal aangeven wat de moeilijkheidsgraad is om de measure te automatiseren in een deployment pipeline.

Tijdens de interviews is gebleken dat de respondenten bij het bepalen of de Information Security Measures eenvoudig te automatiseren zijn voornamelijk hebben gekeken of er al standaard tooling op de markt beschikbaar is om de desbetreffende measure te automatiseren. Daarnaast hebben ze ook gekeken of er al ervaring was met het automatiseren van deze measures binnen een deployment pipeline in hun eigen organisatie.

Automatability	Scale	Manual time	Scale
Very easy	1	1 to 4 hours	5
Easy	2	4 to 8 hours	4
Neither	3	8 to 12 hours	3
Difficult	4	12 to 16 hours	2
Very Difficult	5	16 hours or more	1

Figuur 7: Vijfpunts-Likertschaal

De antwoorden zijn, zoals in figuur 7 aangegeven, omgezet naar schalen, bij elkaar opgeteld en vervolgens gedeeld door de aantal participanten om tot een gemiddelde te kunnen komen.

Tevens is gevraagd aan de experts om aan te geven hoeveel tijd het ongeveer zou kosten als bestaande bewijsmateriaal handmatig verzameld zou worden om aan te tonen dat men aan het desbetreffende Topic voldoet. De tijdsindicatoren die zijn gehanteerd zijn gebaseerd op dagdelen

van een reguliere werkdag van 8 uur. De resultaten hiervan worden niet verder behandeld omdat ze buiten scope zijn geplaatst vanwege verschillende interpretaties van de experts.

De schalen van **Automatability** en **Manual time** lopen tegengesteld omdat dit het sorteren makkelijker zou maken. Door de meest eenvoudige automatiseerbare measure bovenaan te zetten en daar tegenover de meest tijdrovende measure om handmatig bewijsmateriaal te verzamelen kunnen organisaties snel inzicht krijgen in welke measure de meeste waarde oplevert wanneer het geautomatiseerd wordt.

Tabel 15 geeft de Top 5 Information Security Measures weer die volgens de experts het meest eenvoudig zijn om te automatiseren binnen een Deployment Pipeline.

Standard Statement	Explanatory Text	Average Score
Access Control Mechanisms - Password	Principle: Target environments (e.g. business applications, systems or network devices) that are configured with access control mechanisms based on passwords, should require users to provide a valid User ID and password before they can gain access to them. Objective: To prevent unauthorised users from gaining access to password-protected critical or sensitive information, business applications, information systems, networks or computing devices.	1,8
Business Application Register	Principle: Business applications should be recorded in an accurate and up-to-date business application register. Objective: To record important information about business applications that can be used to support information risk assessments, compare relative risks between applications and identify unauthorised applications.	2
Installation Process	Principle: New systems should be installed in the live environment in accordance with a documented installation process. Objective: To minimise disruption to the organisation when new systems are installed in the live environment.	2
Change Management	Principle: Changes to business applications, information systems and network devices should be tested, reviewed and applied using a change management process. Objective: To ensure that changes are applied correctly and do not compromise the security of business applications, computer systems or networks.	2,2
Information Classification and Handling	Principle: An information classification scheme should be established (supported by information handling guidelines) that applies throughout the organisation, based on the confidentiality of information. Objective: To ensure that information is protected in line with its assigned level of classification.	2,2

Tabel 15: Top 5 meest eenvoudige automatiseerbare Information Security Measures

Tabel 16 geeft de Top 5 Information Security Measures weer die volgens de experts het meest moeilijk zijn om te automatiseren binnen een Deployment Pipeline.

Standard Statement	Explanatory Text	Average Score
Information Security Function	Principle: A specialist information security function should be established, which has responsibility for promoting information security throughout the organisation. Objective: To ensure good practice in information security is applied effectively and consistently throughout the organisation.	5
Business Continuity Strategy	Principle: A business continuity strategy covering the whole organisation should be established, which promotes the need for business continuity management, embeds business continuity management into the organisation's culture, and is implemented in the form of a business continuity programme. Objective: To align business continuity goals with the organisation's business goals, provide resilience against disruption and minimise impact to the organisation in the event of a disaster or emergency.	4,8
Crisis Management	Principle: A crisis management process should be established, supported by a crisis management team, which details actions to be taken in the event of a major incident or serious attack. Objective: To respond to major incidents and serious attacks quickly and effectively, reducing any potential business impact including brand and reputational damage.	4,8
Physical Protection	Principle: All critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) should be physically protected against accident or attack and unauthorised physical access. Objective: To restrict physical access to authorised individuals, ensure that critical facilities are available when required and to prevent important services from being disrupted by loss of, or damage to, equipment or services.	4,8
Business Continuity Programme	Principle: A business continuity programme should be established, which includes developing a resilient technical infrastructure, creating a crisis management capability, and coordinating and maintaining business continuity plans and arrangements across the organisation. Objective: To enable the organisation to withstand the prolonged unavailability of critical information, business applications and related technical infrastructure, and provide individuals with a documented set of actions to perform in the event of a disaster or emergency.	4,7

Tabel 16: Top 5 meest moeilijke automatiseerbare Information Security Measures

In bijlage 4 is de ruwe data lijst opgenomen met de gegeven antwoorden per respondent.

In bijlage 6 is de framework opgenomen dat op volgorde laat zien welke Information Security Measures eenvoudig of moeilijk geautomatiseerd kunnen worden in een Deployment Pipeline. Deze Information Security Measures zijn onderverdeeld in drie categorieën:

Categorie	Regel
Easy to automate	3 of meer antwoorden met very easy of easy
Difficult to automate	3 of meer antwoorden met very difficult of difficult
Needs more investigation	3 of meer antwoorden met neither of antwoorden die ver van elkaar afliggen

Tabel 17: Categorisering resultaten

Op de vraag welke Information Security Measures geautomatiseerd zijn binnen hun eigen organisatie, worden voornamelijk de technische measures genoemd en een paar procesmatige checks.

Enkele respondenten vinden ISF een goed framework om de kaders vast te stellen waarbinnen je als bedrijf wilt opereren, omdat dit een vrij compleet framework is. Echter geven de meeste respondenten aan dat voor het automatiseren binnen een deployment pipeline het ISF framework erg ambiteus is, omdat het vrij hoog over is en dat het nog concreet gemaakt moet worden om te kunnen automatiseren.

Alle respondenten geven aan dat waar mogelijk het liefst alle Information Security Measures geautomatiseerd moeten worden om meer grip te krijgen en om snel te kunnen aantonen dat je in control bent. Respondent drie geeft aan dat er ook gekeken moet worden naar hoeveel effort het kost en wat het oplevert en respondent vier geeft aan dat bij sommige controls menselijk inzicht wel een meerwaarde kan opleveren, omdat niet alles zwart wit kan zijn.

Uit de resultaten van de interviews blijkt dat de Information Security Measures die gebaseerd zijn op ISF in vier verschillende niveaus gecategoriseerd kunnen worden:

1. Governance measures

Measures die op organisatieniveau geïmplementeerd kunnen worden. Deze measures zijn veelal moeilijk te automatiseren, kan wellicht in workflow tools maar dat is buiten de scope omdat dit onderzoek over Deployment Pipelines gaat

2. Procesmatige measures

Measures die procesmatige checks afvangen in de Deployment Pipelines, bijvoorbeeld het vierogen principe

3. Applicatieve measures

Measures die op applicatie niveau genomen moeten worden en specifiek gemaakt moeten worden per applicatie. Deze zouden dan per applicatie in de Deployment Pipelines wel geautomatiseerd kunnen worden.

4. Infrastructurele measures

Technische measures die eenvoudiger te automatiseren zijn en ook herhaalbaar zijn waar veelal ook standaard tooling voor beschikbaar is zoals vulnerability scans, code quality review etc.

5. Conclusie, discussie en aanbevelingen, reflectie

Dit hoofdstuk bevat ten eerste een discussie van de resultaten en de daarbij behorende conclusies. Ten tweede worden er aanbevelingen gedaan voor de praktijk en voor verder onderzoek en ten derde wordt een reflectie gegeven op de kwaliteit van dit onderzoek en de houdbaarheid van de conclusies.

5.1. Discussie

Interne & externe validiteit

Om de validiteit van dit onderzoek te bevorderen hebben de experts vooraf aan de semi-gestructureerde interviews een uitnodiging ontvangen met daarin uitleg over de thema's en definities over de gehanteerde termen zoals wat wordt verstaan onder "automatisering". Ook het doel van het interview is vooraf bekend gemaakt zodat de experts er alvast over konden nadenken. De semi-gestructureerde interviews hebben plaatsgevonden in afgesloten vergaderkamers zodat externe factoren minimaal konden storen. Tijdens de interviews is gevraagd aan de experts welke criteria ze hebben gehanteerd bij het geven van de antwoorden in kolom L, Automatability? Dit om zeker te zijn dat de experts de vraag op een eenduidige manier beantwoord hebben. Door deze aanpak hebben de antwoorden op kolom L, dat tevens ook antwoord geeft op de centrale vraag, een hoge mate van validiteit.

Echter doordat twee experts tijdens het invullen van de vragenlijst hebben gevraagd hoe kolom M, Manual time? geïnterpreteerd moest worden is geconcludeerd dat de uitleg over Manual time niet duidelijk genoeg was. Doordat de uitleg niet duidelijk genoeg was, is niet gemeten wat gemeten had moeten worden waardoor de interne validiteit voor dit gedeelte laag is en is dit stuk buiten scope geplaatst en niet verder behandeld in dit onderzoek.

Dit onderzoek is uitgevoerd binnen één financiële instelling en met een beperkt aantal respondenten, hierdoor heeft het resultaat van dit onderzoek een lage externe validiteit en kan het beperkt gegeneraliseerd worden.

Betrouwbaarheid

Om gebrek aan standaardisatie bij semi-gestructureerde interviews te voorkomen waardoor de betrouwbaarheid verlaagd zou kunnen worden (Saunders et al., 2015) is een aantal maatregelen genomen. Ten eerste is een proefinterview gehouden met een controle respondent die kennis heeft van dit domein en naar aanleiding van zijn feedback zijn een aantal vragen scherper gedefinieerd en aanvullende vragen toegevoegd. Tevens is vooraf aan de interviews een gestandaardiseerde vragenlijst ingevuld door de zes experts met als doel om antwoord te kunnen geven op deelvraag vier, namelijk welke Information Security Measures geautomatiseerd kunnen worden in een Deployment Pipeline. De vragen zijn zoveel mogelijk open gesteld en de interviews zijn opgenomen en vastgelegd in bijlage 5. Vervolgens zijn de transcripten van de experts naar hun toegestuurd om deze inhoudelijk te valideren. Aan de experts is gevraagd om binnen twee weken inhoudelijk te reageren op hun eigen transcripten. Dit om de experts de mogelijkheid te geven om achteraf nog te kunnen reageren op de antwoorden die ze gegeven hebben.

Vier van de zes experts hebben bevestigend gereageerd en de andere twee hebben geen reactie gegeven. Alhoewel de onderzoeker de transcripten letterlijk heeft overgenomen naar aanleiding van de audio opnamen kan het feit dat twee experts niet hebben gereageerd vooralsnog invloed hebben

op de betrouwbaarheid. Daarnaast zijn de experts allen werkzaam binnen één organisatie, binnen dezelfde sector, in hetzelfde land waardoor de resultaten van dit onderzoek een lagere betrouwbaarheid zouden kunnen hebben.

Repliceerbaarheid

Binnen dit onderzoek is zorgvuldig omgegaan met het documenteren van de zoekkaders en zoektermen die tijdens het literatuuronderzoek zijn gebruikt. De gevonden resultaten tijdens het literatuuronderzoek zijn systematisch in een aparte lijst bijgehouden met de bijhorende URL naar de bron. Deze zijn te vinden in bijlage 1. De vragenlijsten die tijdens de interviews zijn gesteld zijn opgenomen als bijlage 3 en de resultaten uit het empirisch onderzoek zijn zorgvuldig en gedetailleerd gedocumenteerd in de vorm van audio opnamen en verslagen in de vorm van transcripten. De transcripten zijn opgenomen als bijlage 5. De herhaalbaarheid van dit onderzoek zal erg hoog zijn als dezelfde ISF framework uit 2018 als uitgangspunt wordt gehanteerd, binnen een vergelijkbare sector en land onderzoek wordt gedaan en als het binnen een korte tijd herhaald wordt. Dit omdat technologie heel snel veranderd en er wellicht in de toekomst meer tools komen waarmee Information Security Measures sneller geautomatiseerd kunnen worden. Tevens is de sector en land ook een belangrijke factor, dit omdat de sector en land meestal wel bepalend is hoe de mate van digitalisering en automatisering is geregeld binnen de organisaties.

Controleerbaarheid

Om de controleerbaarheid van dit onderzoek te verhogen zijn er meerdere maatregelen genomen. De gehanteerde onderzoeksmethode is uitgebreid gerapporteerd in Hoofdstuk 3. De beperkingen van dit onderzoek zijn beschreven en de gegevens die hebben geleid tot de resultaten en conclusies zijn beschikbaar gesteld, zoals de transcripten (bijlage 5), audio opnamen (opvraagbaar via OU), ingevulde vragenlijsten (bijlage 4) en een duidelijk overzicht van de gevonden literatuur (bijlage 1). Tevens is er een kort cyclische onderzoek begeleiding geweest met de promotor.

Ethische aspecten

De experts zijn voordat het interview begon geïnformeerd over het feit dat hun deelname geheel vrijwillig is en dat ze zonder enige reden mogen terugtrekken uit het onderzoek. Tevens is gevraagd of er een audio opname gemaakt mocht worden en ook duidelijk aangegeven dat ze de audio opname ten alle tijdens mochten stoppen. De anonimiteit van de experts is gewaarborgd door hun namen niet vast te leggen in de transcripten binnen dit onderzoek. Tevens is gelet op dat de geselecteerde respondenten geen directe hiërarchische relatie met de onderzoeker hebben zodat ze zonder aarzelen hun mening vrij konden uiten. De controle respondent waarmee het proefinterview is gehouden heeft wel een directe hiërarchische relatie met de onderzoeker. De eerste begeleider van deze scriptie is tijdens de beginperiode de directe manager geweest van de onderzoeker. Tijdens het afstuderen was dit niet meer het geval.

5.2. Conclusie

De doelstelling van dit onderzoek was het bepalen van welke Information Security Measures geautomatiseerd kunnen worden in het Continuous Delivery softwareontwikkelproces. Om dit te achterhalen is onderzocht welke Information Security Measures op een geautomatiseerde manier binnen een Deployment Pipeline framework geïntegreerd kunnen worden.

De vraag die in dit onderzoek centraal stond was:
Welke Information Security Measures kunnen geautomatiseerd worden binnen de Continuous Deployment Pipeline zodat een Continuous Compliance framework bewerkstelligd kan worden?

Om de centrale vraag te kunnen beantwoorden zijn een aantal deelvragen gesteld waarvan de antwoorden onderzocht zijn in literatuuronderzoek en empirisch onderzoek.

Continuous Compliance Framework

De resultaten van de eerste deelvraag hebben aangetoond dat er in de wetenschappelijke literatuur geen bruikbaar Continuous Compliance Framework bekend is dat toegepast kan worden binnen Deployment Pipelines. Tevens is uit het empirisch onderzoek gebleken dat de geïnterviewde experts niet bekend zijn met een Continuous Compliance Framework. Hiermee kunnen we concluderen dat dit onderzoek een framework naar voren brengt wat gebruikt kan worden in zowel praktijk als theorie. Dit framework is opgenomen in bijlage 6.

Information Security Frameworks in Deployment Pipelines

Uit literatuuronderzoek is geen standaard Information Security Framework gevonden dat gebruikt kan worden in Deployment Pipelines. De experts die geïnterviewd zijn tijdens het empirisch onderzoek hebben aangegeven geen kennis of ervaring te hebben met een Information Security Framework dat geïmplementeerd kan worden in Deployment Pipelines. Volgens de respondenten zijn frameworks meestal holistisch en de Deployment Pipeline is erg technisch en specifiek, waardoor er niet direct een framework voor handen is dat gebruikt kan worden in Deployment Pipelines. De respondenten geven aan dat het ISF framework meer geschikt is voor de waarom en wat vraag en minder voor hoe measures geïmplementeerd kunnen worden. Op basis van deze resultaten kunnen we concluderen dat momenteel geen geschikte Information Security Framework beschikbaar is dat gedetailleerd inzicht geeft in hoe bepaalde security measures geïmplementeerd en geautomatiseerd kunnen worden binnen Deployment Pipelines.

Information Security Measures in Deployment Pipelines

Uit de ingevulde vragenlijst dat is opgenomen in bijlage 4 is gebleken dat de technische measures de meest eenvoudige automatiseerbare soort measures zijn. Hoe minder specifiek een measure is, zoals procesmatige measures of measures op bestuurlijk niveau, hoe moeilijker het is om dit te automatiseren in Deployment Pipelines. Er zijn tools beschikbaar waarmee processen geautomatiseerd kunnen worden, dat wordt niet verder behandeld in dit onderzoek, omdat dit buiten de scope van het onderzoek ligt. Bij het maken van een keuze om welke security measures te automatiseren in Deployment Pipelines, is het raadzaam om eerst te focussen op de specifiekere technische measures omdat die eenvoudiger te automatiseren zijn. In bijlage 4 is de totale lijst opgenomen en is te zien welke measures eenvoudig te automatiseren zijn.

Automatisering van Information Security Measures

Uit de ingevulde vragenlijst die gebaseerd is op het ISF framework is gebleken dat de experts voornamelijk de technisch georiënteerde measures als 'eenvoudig' automatiseerbaar hebben gekozen. Tijdens de interviews is door de experts aangegeven dat het erg ambitieus is om alles van ISF te automatiseren, omdat het erg veel en hoog over is.

In bijlage 4 is een overzicht opgenomen dat antwoord geeft op de centrale vraag van dit onderzoek. In dit overzicht wordt gedetailleerd getoond welke Information Security Measures geautomatiseerd kunnen worden in Deployment Pipelines. Het overzicht dat is opgenomen in bijlage 4 is vertaald naar een Continuous Compliance framework dat is opgenomen in bijlage 6. Dit framework kan als leidraad gebruikt worden om de Information Security Measures in Deployment Pipelines in een bepaalde volgorde te automatiseren. Door in dit onderzoek inzichtelijk te maken welke Information Security Measures geautomatiseerd kunnen worden in een Deployment Pipeline kunnen we concluderen dat uitvoerig antwoord is gegeven op de centrale vraag van dit onderzoek.

5.3. Aanbevelingen voor de praktijk

Tegenwoordig zijn veel organisaties bezig om automatiseringsslagen te maken binnen hun IT-landschap. Het automatiseren van security en compliance is daar een belangrijk onderdeel van als het gaat om bedrijven waar veel toezicht op wordt gehouden. De resultaten uit dit onderzoek kunnen gebruikt worden bij organisaties die op dit compliance vlak willen automatiseren. Het overzicht in bijlage 4 toont een lijst met measures die eenvoudig tot moeilijk geautomatiseerd kunnen worden binnen een deployment pipeline. Zodra organisaties security measures willen automatiseren in hun deployment pipelines, kan deze lijst als input worden gebruikt om roadmaps te prioriteren.

Daarnaast zal het inzicht geven in het ISF framework, omdat alle topics binnen dit onderzoek behandeld zijn en kunnen organisaties een objectieve mening vormen over het ISF framework en toetsen of dit ISF framework binnen hun ambities en organisatie past.

Tevens kan ook gekeken worden naar tooling om het compliance proces te automatiseren en te koppelen aan deployment pipelines. Hiervoor is al een eerste aanzet voor gemaakt en een tool voor ontwikkeld binnen een Nederlandse verzekeringsmaatschappij. Deze tool zorgt ervoor dat de basis security administratie per applicatie is gecentraliseerd in één repository, hiermee behoort het gebruik van spreadsheets tot de verleden tijd. Door ongestructureerde data, dat verspreid was middels spreadsheets over de gehele organisatie, te structureren en te centraliseren is het eenvoudig te koppelen aan deployment pipelines om zo technische maar ook procesmatige checks uit te voeren. Meer informatie over deze tool kan gevonden worden op de website https://www.thelockchain.eu/ waar de conference paper over deze tool ook te vinden is (Bobbert & Ozkanli, 2020).

5.4. Aanbevelingen voor verder onderzoek

Dit onderzoek heeft zich voornamelijk gericht om een overzicht te creëren van Information Security Measures die geautomatiseerd kunnen worden binnen een Deployment Pipeline. Aanbevolen wordt om met een vervolgonderzoek een stap dieper te gaan en bijvoorbeeld één van de Information Security Measures te onderzoeken hoe deze geautomatiseerd kunnen worden binnen een Deployment Pipeline.

Tevens is het aan te bevelen om te onderzoeken hoeveel tijd bespaard kan worden met het automatiseren van Information Security Measures in Deployment Pipelines. Dit is met name interessant omdat men met de bespaarde tijd kan focussen om meer business waarde toe te voegen waar vaak geen tijd voor is vanwege alle verplichtingen waar organisaties aan moeten voldoen. Hiervoor is in dit onderzoek een eerste aanzet gedaan door de respondenten te vragen hoeveel tijd ze denken te besteden als ze de bewijsmateriaal handmatig zouden verzamelen, echter is dit buiten scope geplaatst. Deze resultaten zouden als input gebruikt kunnen worden om een vergelijking te maken tussen de tijdbesteding van het handmatig verzamelen van bewijsmateriaal en het automatisch genereren van bewijsmateriaal in Deployment Pipelines. Dit inzichtelijk maken is met name interessant om de volgorde te bepalen welke Information Security Measures als eerste te automatiseren, waarmee kosten bespaart kunnen worden.

5.5. Reflectie

Terugkijkend op dit onderzoek ben ik erg tevreden met het gekozen onderwerp omdat dit een heel relevant onderwerp is waar nog weinig onderzoek naar is gedaan. Hierdoor leveren de resultaten van dit onderzoek een relevante bijdrage aan de wetenschap en de praktijk.

Om uit te sluiten dat eerder onderzoek is gedaan naar dit onderwerp is het literatuuronderzoek zeer uitgebreid gezocht naar relevante literatuur. Vervolgens was het kiezen van een geschikte onderzoeksmethode voor het empirisch onderzoek in eerste instantie onduidelijk. Voor ik aan het literatuuronderzoek begon wist ik niet welke onderzoeksmethode ik ging kiezen voor het empirische gedeelte. Na het uitwerken van het literatuuronderzoek werd duidelijk dat een ontwerpgericht onderzoek het meest geschikte methode zou zijn voor dit onderzoek.

Tijdens de literatuurstudie heb ik alleen in Engelstalige artikelen gezocht, wellicht was er in andere talen wel relevantere literatuur beschikbaar, maar deze zijn omwille van de tijd buiten scope gelaten. De gevonden artikelen die niet toegankelijk waren of waarvan de URL naar de bron niet werkten heb ik niet mee kunnen nemen in mijn literatuuronderzoek. Daarnaast kunnen sommige conclusies uit bestaande artikelen al verouderd zijn, dit omdat techniek snel verandert. Als het onderzoek op een later moment herhaald zou worden dan zouden de uitkomsten hierdoor anders kunnen zijn.

Het doel van dit onderzoek was om een overzicht te creëren welke Information Security Measures geautomatiseerd kunnen worden in een Deployment Pipeline. Doordat het ISF framework het meest uitgebreide framework is, is er gekozen voor het ISF framework uit 2018.
Zodra een nieuwe versie van ISF wordt uitgebracht zal er aanvullend onderzoek gedaan moeten worden naar de automatiseerbaarheid van de nieuwe of gewijzigde topics. De resultaten en conclusies voor het ISF framework uit 2018 zal zijn houdbaarheid behouden.

Wat erg is opgevallen is dat de verwoording van het ISF standaard erg holistisch is, waardoor er verschillende interpretaties gegeven kan worden aan de betekenis van de topics door de respondenten. Om een compleet beeld te kunnen krijgen heb ik toch gekozen om gebruikt te maken van het ISF topic niveau wat heel hoog over is, terwijl de Deployment Pipeline juist heel erg specifiek is. Ondanks dat de topics hoog over zijn, is er toch een lijst uitgekomen met Information Security Measures die geautomatiseerd kunnen worden. Achteraf gezien had ik wellicht eerst zelf een selectie kunnen maken en op basis daarvan de respondenten vragen om de geselecteerde lijst in te vullen. Nu hebben de respondenten heel veel tijd moeten besteden om de vragenlijst in te vullen waardoor ik het onderzoek niet grootschaliger heb kunnen aanpakken.

In de interviews hebben de respondenten heel veel informatie gegeven, maar ook vaak te veel over minder relevante zaken. Ondanks dat scoping en vraagstelling vooraf duidelijk is gecommuniceerd, namelijk de Deployment Pipeline, heeft het veel moeite gekost om de respondenten gefocust te houden op de scope Deployment Pipeline. Resultaat hiervan is dat meer data beschikbaar is dan in eerste instantie verzameld zou worden. Hiermee zijn veel aanvullende inzichten verkregen, die goed zijn om te weten maar niet direct antwoord geven op de onderzoeksvragen.

Ondanks de uitleg van de termen die vooraf zijn gedeeld met de respondenten is tijdens de interviews toch gebleken dat er andere interpretaties gegeven zijn aan de definitie van “Manual time”. Hierdoor zijn de resultaten hiervan niet betrouwbaar en is besloten om dit stuk uit scope te plaatsen van dit onderzoek. Achteraf gezien was het beter geweest om bij alle respondenten na te gaan hoe ze “Manual time” hebben geïnterpreteerd. Bij respondent 1 is de laatste sub deelvraag helaas niet gesteld en beantwoord, omdat deze per ongeluk niet mee was geprint. Dit had wellicht voorkomen kunnen worden door de eerste interview beter voor te bereiden.

Tot slot kan ik concluderen dat met dit onderzoek een hiaat is opgevuld in de wetenschappelijke literatuur over de automatiseerbaarheid van Information Security Measures in Deployment Pipelines en dat de resultaten hiervan in de praktijk goed bruikbaar zullen zijn.

Referenties

Al-Hashimi, M., Al-Nidawi, W. J., Othman, M., Shakir, M., & Sulaiman, H. (2019). Evaluate Information Security Governance Frameworks in Cloud Computing Environment Using Main and Sub Criteria. *Journal of Computational and Theoretical Nanoscience, 16*(3), 996-1006.

Alnuem, M., Alrumaih, H., & Al-Alshaikh, H. (2015). A comparison study of information security risk management frameworks in cloud computing. *Cloud computing*, 103-109.

Bass, L., Holz, R., Rimba, P., Tran, A. B., & Zhu, L. (2015). *Securing a deployment pipeline.* Paper presented at the Proceedings of the Third International Workshop on Release Engineering.

Bobbert, Y. (2017). Enterprise Engineering in Business Information Security. *EEWC*.

Bobbert, Y., & Mulder, H. (2019). Enterprise Engineering in Business Information Security. *Springer Nature Switzerland AG*.

Bobbert, Y., & Ozkanli, N. (2020). *LockChain Technology as One Source of Truth for Cyber, Information Security and Privacy.* Paper presented at the the Proceedings of 2020 Computing Conference, London.

Chen, H. (2013). *An Information Security Risk Assessment Framework for Cloud Computing.* Paper presented at the Advanced Materials Research.

Chen, L. (2015). Continuous Delivery: Huge Benefits, but Challenges Too. *IEEE Software, 32*(2), 50-54. doi:10.1109/ms.2015.27

Claps, G. G., Svensson, R. B., & Aurum, A. k. (2014). On the journey to continuous deployment: Technical and social challenges along the way. *School of Information Systems, Technology and Management, University of New South Wales, Sydney, Australia*.

De Nederlandse grondwet. (2019). Retrieved from https://www.denederlandsegrondwet.nl

Derksen, B., Neggers, M., Onwezen, D., & Zelen, S. (2018). *Agile Secure Software Lifecycle Management Secure by Agile Design*. Leiden: Secure Software Alliance (SSA.).

Fischl Bodner, E. (2018). 6 Steps for Ensuring Continuous Compliance in a Complex, Hybrid IT Environment. Retrieved from https://www.itbusinessedge.com/slideshows/6-steps-for-ensuring-continuous-compliance-in-a-complex-hybrid-it-environment-09.html

Forsgren, N., Humble, J., & Kim, G. (2018). *Accelerate*: IT Revolution, Portland, Oregon.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*.

Humble, J., & Farley, D. (2010). *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation (Adobe Reader)*: Pearson Education.

Johnson, J. (2015). CHAOS Report. *the Standish Group*.

Koopman, M. (2019). *A framework for detecting and preventing security vulnerabilities in continuous integration/continuous delivery pipelines.* University of Twente,

Lang, U., & Schreiner, R. (2011). Analysis of recommended cloud security controls to validate OpenPMF “policy as a service”. *information security technical report, 16*(3-4), 131-141.

Li, X., Jin, X., Wang, Q., Cao, M., & Chen, X. (2018). SCCAF: A secure and compliant continuous assessment framework in cloud-based IoT context. *Wireless Communications and Mobile Computing, 2018*.

List of Computer Science Journals. (2019). Retrieved from https://en.wikipedia.org/wiki/List_of_computer_science_journals

Long, J. (2015). What is Continuous Compliance and Assurance? Retrieved from http://www.infosecisland.com/blogview/23823-What-is-Continuous-Compliance-and-Assurance.html

Lu, H.-K., Lin, P.-C., Huang, P.-C., & Yuan, A. (2017). *Deployment and Evaluation of a Continues Integration Process in Agile Development* Chinese Culture University, Taipei, Taiwan.

Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security, 20*(4), 248-263.

Negara, E., & Andryani, R. (2014). A Review: Security Framework Information Technology for University Based on Cloud Computing.
Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Elsevier*.
OpenSAMM. (2019). Retrieved from https://www.opensamm.org/
Oppenheim, C., Stenson, J., & Wilson, R. M. S. (2003). Studies on Information as an Asset II: Repertory Grid. *Journal of Information Science & Technology Association/Joho no Kagaku to Gijutsu, Vol 29*(Issue 5), pp 419 - 432.
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*.
Powell, S. G., Baker, K. R., & Lawson, B. (2009). Impact of errors in operational spreadsheets. *Decision Support Systems, 47*(2), 126-132.
Prins, A. (2016). Introductie op Continuous Compliance. Retrieved from http://www.ideetotit.nl/team-activiteit/introductie-op-continuous-compliance/
Rebollo, O., Mellado, D., & Fernández-Medina, E. (2012). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *J. UCS, 18*(6), 798-815.
Recker, J. (2013). *Scientific Research in Information Systems*. New York Dordrecht London: Springer Heidelberg.
Rylander, J., & Moberg, J. (2018). Automated Key Rotations In a Continuous Deployment Pipeline. In.
Saunders, M., Lewis, P., & Thornhill, A. (2015). *Methoden en technieken van onderzoek* (7e editie ed.). Amsterdam: Pearson.
Schinagl, S., Paans, R., & Schoon, K. (2016). *The revival of ancient information security models, insight in risks and selection of measures.* Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS).
Shahin, M., Babar, M. A., & Zhu, L. (2017). Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. *IEEE Access, 5*, 3909-3943.
Sikdar, P. (2011). Alternate Approaches to Business Impact Analysis. *Information Security Journal: A Global Perspective*(20), 128–134. doi:10.1080/19393555.2010.551274
Strauss, A., & Corbin, J. (2008). *Basics of qualitative research (3rd ed.): Techniques and procedures for developing grounded theory.*: Thousand Oaks, CA: SAGE Publications.
Tariq, M. I. (2012a). *INFORMATION SECURITY METRICS FRAMEWORK FOR CLOUD COMPUTING.* Paper presented at the 9th International Conference on Statistical Sciences.
Tariq, M. I. (2012b). Towards information security metrics framework for cloud computing. *International Journal of Cloud Computing and Services Science, 1*(4), 209.
Tariq, M. I., Haq, D., & Iqbal, J. (2013). SLA Based Information Security Metric for Cloud Computing from COBIT 4.1 Framework. *International Journal of Computer Networks and Communications Security, 1*(3), 95-101.
Tariq, M. I., Tayyaba, S., Hashmi, M. U., Ashraf, M. W., & Mian, N. A. (2017). Agent Based Information Security Threat Management Framework for Hybrid Cloud Computing. *IJCSNS, 17*(12), 57.
The Institute of International Auditors. (2019). Retrieved from https://na.theiia.org/Pages/IIAHome.aspx
Ullah, F., Raft, A. J., Shahin, M., Zahedi, M., & Babar, M. A. (2017). Security support in continuous deployment pipeline. *arXiv preprint arXiv:1703.04277*.
Vedani, J., & Ramaharobandro, F. (2013). Continuous compliance: a proxy-based monitoring framework. *arXiv preprint arXiv:1309.7222*.
Verschuren, P., & Doorewaard, H. (2007). *Het ontwerpen van een onderzoek*: Boom Lemma Uitgevers.

Visser, J., Rigal, S., van der Leek, R., van Eck, P., & Wijnholds, G. (2016). *Building Maintainable Software*: O'Reilly Media Inc.
Weill, P., & Woerner, S. L. (2015). Thriving in an Increasingly Digital Ecosystem. *Massachusetts Institute of Technology, Vol. 56, No. 4*.
Zeni, N., Kiyavitskaya, N., Mich, L., Cordy, J. R., & Mylopoulos, J. (2013). GaiusT: supporting the extraction of rights and obligations for regulatory compliance. *Springer-Verlag London*.
Zitting, D. (2015). Are You Still Auditing in Excel? *Sarbanes Oxley Compliance Journal*. Retrieved from http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=4156

Figurenlijst

Figuur 1: Basic Deployment Pipeline (Humble & Farley, 2010) 4
Figuur 2: Aanpak onderzoeksmodel 8
Figuur 3: Fases van het zoekproces 10
Figuur 4: Agile Software Assurance Maturity Model (ASAMM, copyright SSA). 21
Figuur 5: Doel empirisch onderzoek 28
Figuur 6: DSRM proces model volgens Peffers et al., (2007) 30
Figuur 7: Vijfpunts-Likertschaal 41

Tabellenlijst

Tabel 1: Zoektermen die gehanteerd zijn tijdens het literatuuronderzoek 11
Tabel 2: Zoekresultaten deelvraag 1 13
Tabel 3: Zoekresultaten deelvraag 2 15
Tabel 4: Zoekresultaten Deelvraag 3 17
Tabel 5: Zoekresultaten deelvraag 4 19
Tabel 6: Information Security Frameworks in Cloud omgevingen 22
Tabel 7: Security Risks in Key Componenten van CDP volgens Ullah et.al. (2017) 24
Tabel 8: Vergelijking van de drie deployment pipelines volgens Rylander and Moberg (2018) 26
Tabel 9: Peffers et al. (2007) versus Verschuren & Doorewaard (2007) 31
Tabel 10: Procedure om experts te selecteren volgens Okoli & Pawlowski (2004) 32
Tabel 11: Interviewvragen en opgeleverde kennis 34
Tabel 12: Categorisering experts 35
Tabel 13: Ethische aspecten (Saunders, 2016) 38
Tabel 14: Overzicht expertinterviews 39
Tabel 15: Top 5 meest eenvoudige automatiseerbare Information Security Measures 42
Tabel 16: Top 5 meest moeilijke automatiseerbare Information Security Measures 43
Tabel 17: Categorisering resultaten 44

Bijlage 1 - Zoekresultaten literatuuronderzoek

Legenda van bijlage 1.1 t/m 1.4:

Kolom	Betekenis
Resultaten	Aantal gevonden resultaten met de gegeven zoekopdracht
Relevantie	Voor welke DV de zoekopdracht relevant is
Zoekbron	Primaire zoekmachines waar de eerste zoekopdracht is gegeven
Datum	Datum van raadplegen van het artikel
Zoekmethode	Systematisch zoeken, sneeuwbal methode, citatiezoeken, forward zoeken etc.
Zoekterm	Gebruikte zoektermen, dit kunnen combinaties zijn van meerdere termen
Zoekkader	Gegeven kaders aan de zoektermen, zoals bijv een specifiek jaartal
Titel artikel	Titel van de gevonden artikel
Auteur(s)	Auteurs van de gevonden artikel
Jaar	Jaartal wanneer het artikel is gepubliceerd
Relevantie titel	Beoordeling of de titel van het artikel voldoet aan de gegeven zoektermen
Relevantie content	Beoordeling van de inhoud van het artikel of het antwoord geeft op de gestelde deelvraag
Gevonden op	Bron waar het artikel is uiteindelijk gevonden
URL	Link naar het gevonden artikel
Aantekeningen	Aantekeningen, opmerkingen die relevant kunnen zijn bij het herhalen van de zoekopdrachten
X	Artikelen die gevonden worden door de zoekmachines maar inhoudelijk niet toegankelijk zijn en daardoor niet beoordeeld kunnen worden op relevantie of artikelen die meerdere keren zijn gevonden

Bijlage 1.1 - Zoekresultaten deelvraag 1

#	Relevantie	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
1	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	Mastering the Journey to Continuous Compliance	Kimberly Hanna; Judy Duvall; Rebecca L. Turpin; More...	2016	Ja	Nee	Sage journals		https://journals.sagepub.com/doi/10.1177/2158244016656231
2	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	A reliable incremental method of computing the limit load in deformation plasticity based on compliance: Continuous and discrete setting	Haslinger, Jaroslav; Repin, Sergey; Sysala, Stanislav	2016	Nee	Nee	ScienceDirect		https://www-sciencedirect-com.ezproxy.elib11.ub.unimaas.nl/science/article/pii/S0377042716300917?via%3Dihub
3	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	Continuous disclosure compliance: does corporate governance matter?	Chapple, Larelle; Truong, Thu Phuong; Cahan, Steven	2015	Nee	Nee	Wiley Online Library		https://onlinelibrary-wiley-com.ezproxy.elib11.ub.unimaas.nl/doi/full/10.1111/acfi.12071
4	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	Causes of non-compliance to continuous positive airway pressure - CPAP-treatment	Ramazanova, A; Durao, V; Fonseca, J; More...	2016	Nee	Nee	Wiley Online Library		niet beschikbaar
5	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	Accurate approximations of concrete creep compliance functions based on continuousretardation spectra	Jirásek, M; Havlásek, P	2014	Nee	Nee	ScienceDirect		https://www.sciencedirect.com/science/article/abs/pii/S0045794914000352
6	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	Random crossover comparison of the effects on sleep disordered breathing related symptoms between mandibular advancement device with compliance monitor and conti...	Yamamoto, U; Soda, S; Handa, S; More...	2016	Nee	Nee	Wiley Online Library		niet beschikbaar
7	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	CONTINUOUS POSITIVE AIRWAY PRESSURE (CPAP) COMPLIANCE AND CONTROL OF OBSTRUCTIVE SLEEP APNOEA (OSA) USING A HOME-BASED AUTO-TITRATION...	Tee, V; Fon, A; Manoharan, B; More...	2016	Nee	Nee	Wiley Online Library		niet beschikbaar
8	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	On the effect of fiber creep-compliance in the high-temperature deformation of continuous fiber-reinforced ceramic matrix composites	Baxevanis, Theocharis; Plexousakis, Michael	2010	Nee	Nee	ScienceDirect		https://www.sciencedirect.com/science/article/pii/S0020768310001770
9	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	Assessment of compliance of dimensional tolerances in concrete slabs using TLS data and the 2D continuous wavelet transform	Puri, Nisha; Valero, Enrique; Turkan, Yelda; More...	2018	Nee	Nee	ScienceDirect		https://www.sciencedirect.com/science/article/abs/pii/S0926580518304400
10	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance	Titel + sinds 01-01-2010, Scholarly & Peer-Reviewed, -((TitleCombined:(continuous compliance))) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (patients)	Establishing continuous relaxation spectrum based on complex modulus tests to construct relaxation modulus master curves in compliance with linear viscoelastic theory	Liu, Hanqi; Luo, Rong; Lv, Huijie	2018	Nee	Nee	ScienceDirect		https://www.sciencedirect.com/science/article/abs/pii/S0950061817326090
11	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Efficient parallel reasoning on fuzzy goal models for run time requirements verification	Chatzikonstantinou, George; Kontogiannis, Kostas	2018	Nee	Nee	SpringerLink		https://link.springer.com/article/10.1007/s10270-016-0562-9
12	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	SCCAF: A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context	Li, X; Jin, X; Wang, QX;	2018	Ja	Nee	Hindawi		https://www.hindawi.com/journals/wcmc/2018/3078272/

#	Relevantie	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
13	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	TOWARDS SUSTAINABILITY THROUGH GREEN, LEAN AND SIX SIGMA INTEGRATION AT SERVICE INDUSTRY: REVIEW AND FRAMEWORK	Caiado, Rodrigo; Nascimento, Daniel; Quelhas, Osvaldo	2018	Nee	Nee	DOAJ		https://www.doaj.org/article/f5cc727861ad43a0ab665937d311c02c
14	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Non-compliance Mechanisms: Interaction between the Kyoto Protocol System and the European Union	Tabau, AS; Maljean-Dubois, S	2010	Nee	Nee	Oxford academic		https://academic.oup.com/ejil/article/21/3/749/508666
15	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Codesign of controller, routing and scheduling in WirelessHART networked control systems	Di Girolamo, Giovanni Domenico; D'Innocenzo, Alessandro	2019	Nee	Nee	Wiley Online Library		https://onlinelibrary.wiley.com/doi/abs/10.1002/rnc.4491
16	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	On the effect of fluid-structure interactions and choice of algorithm in multi-physics topology optimisation	Munk, David J; Kipouros, Timoleon; Vio, Gareth A;	2018	Nee	Nee	ScienceDirect	2 keer gevonden als resultaat in zelfde zoekmachine	https://www.sciencedirect.com/science/article/abs/pii/S0168874X17308272
17	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	NEGOSEIO: A framework for negotiations toward Sustainable Enterprise Interoperability	Cretan, Adina; Coutinho, Carlos; Bratu, Ben	2012	Nee	Nee	ScienceDirect		https://www.sciencedirect.com/science/article/pii/S1367578812000454
18	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	AMPLE: an anytime planning and execution framework for dynamic and uncertain problems in robotics	Ponzoni Carvalho Chanel, Caroline; Albore, Alexandre; T'Hooft, Jorrit	2019	Nee	Nee	SpringerLink		https://link.springer.com/article/10.1007/s10514-018-9703-z
19	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Conceptualising cosmopolitanism and entrepreneurship through the lens of the three-dimensional theory of power	Mouraviev, Nikolai; Kakabadse, Nada K	2016	Nee	Nee	Emerald insight		https://www.emerald.com/insight/content/doi/10.1108/SBR-12-2015-0071/full/html
20	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Multiple continuity of phases in composite materials: Overall property estimates from a laminate system scheme	Franciosi, P	2019	Nee	Nee	ScienceDirect		https://www.sciencedirect.com/science/article/abs/pii/S0020768319301027
21	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Design of variable stiffness composite structures using lamination parameters with fiber steering constraint	Demir, Eralp; Yousefi-Louyeh, Pouya; Yildiz, Mehmet	2019	Nee	Nee	ScienceDirect		https://www.sciencedirect.com/science/article/abs/pii/S1359836818336631
22	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Nonlinear filters in topology optimization: existence of solutions and efficient implementation for minimum compliance problems	Hägg, Linus; Wadbro, Eddie	2017	Nee	Nee	SpringerLink		https://link.springer.com/article/10.1007/s00158-016-1553-8
23	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Organizing and running winter triathlon competitions in Ukraine	Vladimir Vodlozerov	2017	Nee	Nee	DOAJ		https://www.doaj.org/article/af295dba93574f8e867e20abfcf6e336
24	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Framing the development and directions of business sustainability efforts	Høgevold, Nils M; Svensson, Göran	2016	Nee	Nee	Emerald insight		https://www.emerald.com/insight/content/doi/10.1108/CG-11-2015-0148/full/html
25	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Process-Property Relationship for Air Plasma-Sprayed Gadolinium Zirconate Coatings	Dwivedi, Gopal; Tan, Yang; Viswanathan, Vaishak	2015	Nee	Nee	SpringerLink		https://link.springer.com/article/10.1007/s11666-014-0196-9
26	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	On the Structural Shape Optimization through Variational Methods and Evolutionary Algorithms	Fraternali, Fernando; Marino, Andrea; Sayed, Tamer El;	2011	Nee	Nee	Taylor&Francis Online		https://www.tandfonline.com/doi/abs/10.1080/15376494.2010.483319
27	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Performance Assessment Model for Municipal Solid Waste Management Systems: Development and Implementation	AlHumid, Hatem; Haider, Husnain; AlSaleem, Saleem;	2019	Nee	Nee	DOAJ		https://www.doaj.org/article/ff25ec45e07b4deb890beffb8cd0484d
28	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Innovation Determinants and Barriers: A Tri-Perspective Analysis of IT Appropriation within an Early Childhood Education and Care Organisation	Plumb, Melinda; Kautz, Karlheinz	2015	Nee	Nee	Australasian Journal of Information Systems		https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1811&context=buspapers

#	Relevantie	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
29	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Auditing in enterprise system environment: a synthesis	Kanellou, Alexandra; Spathis, Charalambos	2011	Nee	Nee	Emerald insight		https://www.emerald.com/insight/content/doi/10.1108/17410391111166549/full/html?queryID=35%2F54077714
30	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	PRAXIOCENTRALISM IN THE PROFESSIONAL STANDARD OF THE TEACHER (Continuation of the article)	L. Yu. Monakhova; V. S. Fedotova	2017	Nee	Nee	DOAJ	2 keer gevonden als resultaat in zelfde zoekmachine	https://www.doaj.org/article/cb46b9ceb3fb436c871c706f967c5bbd
31	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	ON DISCRETE STRUCTURE OF GEOLOGIC MEDIUM AND CONTINUAL APPROACH TO MODELING ITS MOVEMENTS	Mukhamediev, Sh. A	2016	Nee	Nee	DOAJ		https://www.doaj.org/article/8f2d302c698b4ad4bd835e9c33ce61e7
32	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Is quality of higher educational institutions in Western Balkan real?	Zivaljevic, Aleksandra; Vrcelj, Nikolina; Tosovic-Stevanovic, Aleksandra	2015	Nee	Nee	Researchgate		https://www.researchgate.net/profile/Aleksandra_Zivaljevic/publication/279166881_Is_quality_of_higher_educational_institutions_in_Western_Balkan_real/links/53527060f7e9b10d845073d/Is-quality-of-higher-educational-institutions-in-Western-Balkan-real.pdf
33	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Online and Offline Trend Cluster Discovery in Spatially Distributed Data Streams	Ciampi, Anna; Appice, Annalisa; Malerba, Donato	2011	Nee	Nee	SpringerLink		https://link.springer.com/chapter/10.1007/978-3-642-23599-3_8
34	DV1	OU bibliotheek	06/07/2019	Systematisch	Continuous Compliance framework	(Abstract:(continuous compliance framework)) NOT (drug) NOT (medical) NOT (medicine) NOT (health) NOT (medical) NOT (water)	Applications of Distributed and Parallel Computing in the Solvency II Framework: The DISAR System	Castellani, Gilberto; Passalacqua, Luca	2011	Nee	Nee	SpringerLink		https://link.springer.com/chapter/10.1007/978-3-642-21878-1_51
35	DV1	Google Scholar	06/07/2019	Systematisch	Continuous Compliance framework	allintitle: continuous compliance framework -drug -medical -medicine -patients -health	Continuous compliance: a proxy-based monitoring framework	Julien Vedani (SAF), Fabien Ramaharobandro	2013	Ja	Nee	Cornell University		arxiv.org/abs/1309.7222

Bijlage 1.2 - Zoekresultaten deelvraag 2

#	Relevantie DV	Datum	Zoekbron	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
1	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Frameworks AND Cloud	Titel, sinds 2010	A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment	O Rebollo, D Mellado, E Fernández-Medina	2012	Ja	Ja	semanticscholar		jucs.org/jucs_18_6/a_systematic_review_of/jucs_18_06_0798_0815_rebollo.pdf
2	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Frameworks AND Cloud	Titel, sinds 2010	A comparison study of information security risk management frameworks in cloud computing	M Alnuem, H Alrumaih, H Al-Alshaikh	2015	Ja	Ja	Researchgate		ieeexplore.ieee.org/abstract/document/7100305
3	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Frameworks AND Cloud	Titel, sinds 2010	Qualitative analysis of various information security frameworks and their newly proposed improvised versions for cloud platform	S Sharma, B Bhushan, S Sharma	2015	Nee	Nee	IEEE xplore		ieeexplore.ieee.org/abstract/document/7100305
4	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Frameworks AND Cloud	Titel, sinds 2010	INFORMATION SECURITY GOVERNANCE FRAMEWORKS IN CLOUD COMPUTING AN OVERVIEW	M Al-hashimi, M Othman, H Sulaiman	2019	Ja	Ja	Researchgate		www.ingentaconnect.com/content/asp/jctn/2019/00000016/00000003/art00033
5	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Frameworks AND Cloud	Titel, sinds 2010	An Overview Of Information Security Governance Frameworks In Cloud Computing	M Shakir, WAR Abu-Ulbeh	2017	Ja	X	Academia	Link werkt niet, ook niet te vinden op Erasmus bibliotheek	
6	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Frameworks AND Cloud	Titel, sinds 2010	Evaluate Information Security Governance Frameworks in Cloud Computing Environment Using Main and Sub Criteria	M Al-Hashimi, WJ Al-Nidawi, M Othman	2019	Ja	X	ingentaconnect	Betaalde artikel, ook niet te vinden op Erasmus bibliotheek	www.ingentaconnect.com/content/asp/jctn/2019/00000016/00000003/art00033
7	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Frameworks AND Cloud	Titel, sinds 2010	On Security of Information Access for Multi Expert Cloud Frameworks	S Naseera, G Gopichand	2018	Nee	Nee	proquest		search.proquest.com/openview/31f248022214414388a52006adce5f77/1?pq-origsite=gscholar&cbl=2042733
8	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Information security risk management framework for the cloud computing environments	X Zhang, N Wuwong,	2010	Ja	X	IEEE xplore	Betaalde artikel, ook niet te vinden op Erasmus bibliotheek	ieeexplore.ieee.org/abstract/document/5577860
9	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Empirical evaluation of a cloud computing information security governance framework	O Rebollo, D Mellado, E Fernández-Medina	2015	Ja	Nee	Elsevier		www.sciencedirect.com/science/article/abs/pii/S0950584914002146
10	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology	R Kalaiprasath, R Elankavi	2017	Nee	Nee	Researchgate		www.researchgate.net/profile/Kalaiprasath_r/publication/317217403_Cloud_Information_Accountability_CIA_framework_ensuring_accountability_of_data_in_cloud_and_security_in_end_to_end_process_in_cloud_terminology/links/5ae159ed458515c60f65fdda/Cloud-Information-Accountability-CIA-framework-ensuring-accountability-of-data-in-cloud-and-security-in-end-to-end-process-in-cloud-terminology.pdf
11	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Towards information security metrics framework for cloud computing	MI Tariq	2012	Ja	Ja	Researchgate		www.researchgate.net/profile/Muhammad_Tariq26/publication/236584581_Towards_Information_Security_Metrics_Framework_for_Cloud_Computing/links/00b7d5181245093bdb000000/Towards-Information-Security-Metrics-Framework-for-Cloud-Computing.pdf
12	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Security policy enforcement framework for cloud-based information processing systems	AM Oprea, Y Zhang, V Ganti, JP Field, A Juels	2014	Ja	Nee	googleapis		patents.google.com/patent/US8689282B1/en
13	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	A new framework for cloud storage confidentiality to ensure information security	D Singh, HK Verma	2016	Nee	Nee	IEEE xplore		ieeexplore.ieee.org/abstract/document/7570933
14	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	SLA Based Information Security Metric for Cloud Computing from COBIT 4.1 Framework	MI Tariq, DIU Haq, J Iqbal	2013	Ja	Ja	Academia		s3.amazonaws.com/academia.edu.documents/31815139/SLA_Based_Information_Security_Metrics_for_Cloud_Computing_from_COBIT_4.1_Framework.pdf?response-content-disposition=inline%3B%20filename%3DSLA_based_Information_Security_Metrics_i.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190804%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190804T151052Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=6283f27b6fecbfe40ba0861f42455c2fb976c4e9d6588fc8c28809f629a2eae3

#	Relevantie DV	Datum	Zoekbron	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
15	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	An efficient framework for information security in cloud computing using auditing algorithm shell (AAS)	MO Mushtaq, F Shahzad, MO Tariq, M Riaz	2017	Ja	Nee	Arxiv		arxiv.org/abs/1702.07140
16	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	An SDN based framework for guaranteeing security and performance in information-centric cloud networks	U Ghosh, P Chatterjee, D Tosh, S Shetty	2017	Nee	Nee	Researchgate		ieeexplore.ieee.org/abstract/document/8030664
17	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	A framework for cloud forensics evidence collection and analysis using security information and event management	M Irfan, H Abbas, Y Sun, A Sajid	2016	Ja	Nee	wiley		onlinelibrary.wiley.com/doi/full/10.1002/sec.1538
18	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	A Review: Security Framework Information Technology for University Based on Cloud Computing	ES Negara, R Andryani	2010	Ja	Ja	binadarma		eprints.binadarma.ac.id/1988/
19	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Agent Based Information Security Threat Management Framework for Hybrid Cloud Computing	MI Tariq, S Tayyaba, MU Hashmi, MW Ashraf, NA Mian	2017	Ja	Ja	Researchgate		www.researchgate.net/profile/Muhammad_Tariq26/publication/323113792_Agent_Based_Information_Security_Threat_Management_Framework_for_Hybrid_Cloud_Computing/links/5a8050ada6fdcc0d4bac2f90/Agent-Based-Information-Security-Threat-Management-Framework-for-Hybrid-Cloud-Computing.pdf
20	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	A strongly trusted integrity preservance based security framework for critical information storage over cloud platform	S Sharma	2016	Ja	Nee	Ijais		www.ijais.org/archives/volume11/number6/sharma-2016-ijais-451612.pdf
21	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	A Cloud Governance Framework for Cloud Computing: an information security governance perspective to protect cloud users	R Ahmad	2013	Ja	Nee	auckland		researchspace.auckland.ac.nz/handle/2292/22205
22	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also ...	IP Chochliouros, AS Spiliopoulou	2015	Nee	Nee	acm		dl.acm.org/citation.cfm?id=2797146
23	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Fraud threats disclosure through cloud information security framework	T Mavroeidakos, DD Vergados	2017	Ja	X	IEEE xplore	Betaalde artikel, ook niet te vinden op Erasmus bibliotheek	ieeexplore.ieee.org/abstract/document/8316457
24	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	An Information Security Risk Assessment Framework for Cloud Computing	H Chen	2013	Ja	Ja	scientific		www.scientific.net/AMR.756-759.1469.pdf?casa_token=cH6hPvwg2rwAAAAA:3YHsitGP9XJsXNKg_HL-sNf0o7ILbUpV01nu5LC3WFXlJ2YWU0GW8TBHzulRBIpdMYh3diSXfEA
25	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	INFORMATION SECURITY METRICS FRAMEWORK FOR CLOUD COMPUTING	MI Tariq	2012	Ja	Ja	Academia		s3.amazonaws.com/academia.edu.documents/31673255/Proc_9th_conf.pdf?response-content-disposition=inline%3B%20filename%3DDesigning_Software_Maintenance_Service_L.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190804%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190804T151515Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=22cbbbcd3150c5bfc54bfde617dfaf9bb1ceb22a89e85f74900cb9715350a5cd#page=327
26	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Efficient Framework for Ensuring the Effectiveness of Information Security in Cloud Computing	LIU Xiao-hui	2014	Nee	Nee	cnki		en.cnki.com.cn/Article_en/CJFDTotal-SDDZ201403052.htm
27	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Information Security Risk Assessment Framework for Cloud Computing Environment Using Medical Research Design and Method	GN Samy, B Shanmugam, N Maarop	2018	Ja	X	ingentaconnect	Betaalde artikel, ook niet te vinden op Erasmus bibliotheek	www.ingentaconnect.com/content/asp/asl/2018/00000024/00000001/art00211
28	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	Information of Public Security Traffic cloud platform framework	XK Sang, WW Ma	2014	Nee	Nee	atlantis-press		www.atlantis-press.com/proceedings/mce-14/14095
29	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	A Context Establishment Framework for Cloud Computing Information Security Risk Management Based on the STOPE View.	BS Alghamdi, M Elnamaky, MA Arafah	2019	Ja	Nee	femto		ijns.femto.com.tw/contents/ijns-v21-n1/ijns-2019-v21-n1-p166-176.pdf
30	DV 2	31/07/2019	Google Scholar	Systematisch	Information Security Framework AND Cloud	Titel, sinds 2010	IMPLEMENT OF SECURITY FOR COMMON PRIVATE DATA IN THE CLOUD USING SCATTER INFORMATION COUNTABILITY FRAMEWORK	P VENKATESWARLU	2015	Nee	Nee	dsresearchcenter		dsresearchcenter.net/PDF/V1_I8/V1-I8-34.pdf

#	Relevantie DV	Datum	Zoekbron	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
31	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Empirical evaluation of a cloud computing information security governance framework	Oscar Rebollo, Daniel Mellado, Eduardo Fernández-Medina, Haralambos Mouratidis	2015	Ja	X	Elsevier	Zelfde artikel als regel 9. Hier wordt Framework en Frameworks gecombineerd uitgewerkt omdat de database zoekt naar 'framework'	www.sciencedirect.com/science/article/pii/S0950584914002146
32	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Empirical evaluation of a cloud computing information security governance framework	Oscar Rebollo, Daniel Mellado, Eduardo Fernández-Medina, Haralambos Mouratidis	2015	Ja	X	Elsevier	Zelfde artikel als regel 9.	www.sciencedirect.com/science/article/pii/S0950584914002146
33	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Empirical evaluation of a cloud computing information security governance framework	Oscar Rebollo, Daniel Mellado, Eduardo Fernández-Medina, Haralambos Mouratidis	2015	Ja	X	Elsevier	Zelfde artikel als regel 9.	www.sciencedirect.com/science/article/pii/S0950584914002146
34	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A framework of cloud-based virtual phones for secure intelligent information management	Jiun-Hung Ding, Roger Chien, Shih-Hao Hung, Yi-Lan Lin, Che-Yang Kuo, Ching-Hsien Hsu, Yeh-Ching Chung	2014	Nee	Nee	Elsevier		www.sciencedirect.com/science/article/pii/S0268401213001515
35	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A framework for cloud forensics evidence collection and analysis using security information and event management	Muhammad Irfan, Haider Abbas, Yunchuan Sun, Anam Sajid, Maruf Pasha	2016	Ja	X	wiley	Zelfde artikel als regel 17.	onlinelibrary.wiley.com/action/doSearch?field1=Title&text1=A+framework+for+cloud+forensics+evidence+collection+and+analysis+using+security+information+and+event+management&field2=Contrib&text2=&field3=AllField&text3=&Ppub=&
36	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A framework for cloud forensics evidence collection and analysis using security information and event management	Muhammad Irfan, Haider Abbas, Yunchuan Sun, Anam Sajid, Maruf Pasha	2016	Ja	X	wiley	Zelfde artikel als regel 17.	onlinelibrary.wiley.com/action/doSearch?field1=Title&text1=A+framework+for+cloud+forensics+evidence+collection+and+analysis+using+security+information+and+event+management&field2=Contrib&text2=&field3=AllField&text3=&Ppub=&
37	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A framework for establishing trust in Cloud provenance	Imad M Abbadi	2013	Nee	Nee	springer		link.springer.com/article/10.1007%2Fs10207-012-0179-0
38	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Taking back control of privacy: a novel framework for preserving cloud-based firewall policy confidentiality	Tytus Kurek, Marcin Niemiec, Artur Lason	2016	Nee	Nee	springer		link.springer.com/search?dc.title=Taking+back+control+of+privacy-&date-facet-mode=between&facet-start-year=2016&dc.creator=kurek&showAll=true
39	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A secure data sharing and query processing framework via federation of cloud computing	Bharath K Samanthula, Yousef Elmehdwi, Gerry Howser, Sanjay Madria	2015	Nee	Nee	Elsevier		www.sciencedirect.com/science/article/pii/S0306437913001208
40	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter	Gandikota Ramu	2018	Nee	Nee	springer		link.springer.com/article/10.1007%2Fs10639-018-9713-7
41	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing	Rajendra Patil, Harsha Dudeja, Chirag Modi	2019	Nee	Nee	springer	2 keer gevonden als resultaat in zelfde zoekmachine	link.springer.com/search?dc.title=Designing+in-VM-assisted+lightweight+agent-based+malware+detection+framework+for+securing+virtual+machines+in+cloud+computing&date-facet-mode=between&facet-start-year=2019&dc.creator=patil&showAll=true
42	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing	Rajendra Patil, Harsha Dudeja, Chirag Modi	2019	Nee	Nee	springer	2keer gevonden als resultaat in zelfde zoekmachine	link.springer.com/search?dc.title=Designing+in-VM-assisted+lightweight+agent-based+malware+detection+framework+for+securing+virtual+machines+in+cloud+computing&date-facet-mode=between&facet-start-year=2019&dc.creator=patil&showAll=true
43	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Evaluate information security governance frameworks in cloud computing environment using main and sub criteria	Al-Hashimi M, Al-Nidawi WJ, Othman M, Sulaiman H, Shakir M	2019	Ja	X		Zelfde artikel als regel 6. Betaalde artikel, ook niet te vinden op erasmus bibliotheek. 2 keer gevonden als resultaat in zelfde zoekmachine	
44	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Evaluate information security governance frameworks in cloud computing environment using main and sub criteria	Al-Hashimi M, Al-Nidawi WJ, Othman M, Sulaiman H, Shakir M	2019	Ja	X		Zelfde artikel als regel 6. Betaalde artikel, ook niet te vinden op erasmus bibliotheek. 2 keer gevonden als resultaat in zelfde zoekmachine	

#	Relevantie DV	Datum	Zoekbron	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
45	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Agent Based Information Security Threat Management Framework for Hybrid Cloud Computing	MI Tariq, S Tayyaba, MU Hashmi, MW Ashraf, NA Mian	2017	Ja	X	Researchgate	Zelfde artikel als regel 19.	www.researchgate.net/profile/Muhammad_Tariq26/publication/323113792_Agent_Based_Information_Security_Threat_Management_Framework_for_Hybrid_Cloud_Computing/links/5a8050ada6fdcc0d4bac2f90/Agent-Based-Information-Security-Threat-Management-Framework-for-Hybrid-Cloud-Computing.pdf
46	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A Conceptual Security Framework for Cloud Computing Issues	Shadi A Aljawarneh, Muneer O Bani Yassein	2016	Ja	X	Erasmus bibliotheek	Betaalde artikel, niet verkrijgbaar via erasmus bibliotheek	
47	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Cloud Security Threats and Techniques to Strengthen Cloud Computing Adoption Framework	Nabeel Khan, Adil Al-Yasiri	2016	Nee	Nee	Erasmus bibliotheek	Betaalde artikel, niet verkrijgbaar via erasmus bibliotheek	
48	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A Framework for Protecting Users' Privacy in Cloud	Adesina S Sodiya, Adegbuyi B	2016	Nee	Nee	Erasmus bibliotheek	Betaalde artikel, niet verkrijgbaar via erasmus bibliotheek	
49	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	A secure mobile commerce framework based on community cloud	Hisham Alsaghier	2017	Nee	Nee	Erasmus bibliotheek	Betaalde artikel, niet verkrijgbaar via erasmus bibliotheek	
50	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Cloud	Titel, sinds 2010	Trust delegation-based secure mobile cloud computing framework	NA Lo', ai A Tawalbeh, Fadi Ababneh, Yaser Jararweh, Fahd AlDosari	2017	Nee	Nee	Erasmus bibliotheek	Betaalde artikel, niet verkrijgbaar via erasmus bibliotheek	
51	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Architectural frameworks: defining the structures for implementing learning health systems	Lessard L, Michalowski W, Fung-Kee-Fung M, Jones L, Grudniewicz A	2017	Nee	Nee	ncbi		www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1748-5908%5Bjour%5D+AND+12%5Bvolume%5D+AND+2017%5Bpdat%5D
52	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Architectural frameworks: defining the structures for implementing learning health systems	Lessard L, Michalowski W, Fung-Kee-Fung M, Jones L, Grudniewicz A	2017	Nee	X	ncbi	Zelfde artikel als 51	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1748-5908%5Bjour%5D+AND+12%5Bvolume%5D+AND+2017%5Bpdat%5D
53	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Secure remote health monitoring with unreliable mobile devices	Shin M	2012	Nee	Nee	ncbi		www.ncbi.nlm.nih.gov/pmc/journals/94/
54	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Secure remote health monitoring with unreliable mobile devices	Shin M	2012	Nee	X	ncbi	Zelfde artikel als 53	www.ncbi.nlm.nih.gov/pmc/journals/94/
55	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams	Michael E Edge, Pedro R Falcone Sampaio	2012	Nee	Nee	sciencedirect		www.sciencedirect.com/science/article/pii/S0957417412001637
56	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Using computer decision support systems in NHS emergency and urgent care: ethnographic study using normalisation process theory	Catherine Pope, Susan Halford, Joanne Turnbull, Jane Prichard, Melania Calestani, Carl May	2013	Nee	X	ncbi	Link werkt niet, niet te vinden op erasmus bibliotheek	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1472-6963%5Bjour%5D+AND+13%5Bvolume%5D+AND+1%5Bpage%5D+AND+2013%5Bpdat%5D
57	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	A Categorization Framework for Common Computer Vulnerabilities and Exposures	Zhongqiang Chen, Yuan Zhang, Zhongrong Chen	2010	Nee	Nee	Oxford University		academic.oup.com/comjnl/article/53/5/551/415583
58	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Using computer decision support systems in NHS emergency and urgent care: ethnographic study using normalisation process theory.	Catherine Pope, Susan Halford, Joanne Turnbull, Jane Prichard, Melania Calestani, Carl May	2013	Nee	X	ncbi	Zelfde artikel als 56	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1472-6963%5Bjour%5D+AND+13%5Bvolume%5D+AND+1%5Bpage%5D+AND+2013%5Bpdat%5D
59	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Deployment	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Using computer decision support systems in NHS emergency and urgent care: ethnographic study using normalisation process theory	Catherine Pope, Susan Halford, Joanne Turnbull, Jane Prichard, Melania Calestani, Carl May	2013	Nee	X	ncbi	Zelfde artikel als 56	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1472-6963%5Bjour%5D+AND+13%5Bvolume%5D+AND+1%5Bpage%5D+AND+2013%5Bpdat%5D
60	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	From Editor	Ugur Demiray	2013	Nee	Nee	doaj		doaj.org/article/2cc1c82d70d14c09887afc1b7cefc960
61	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Programme potential for the prevention of and response to sexual violence among female refugees a literature review	Gianna Maxi Leila Robbers, Alison Morgan	2017	Nee	Nee	tandfonline	2 keer gevonden als resultaat in zelfde zoekmachine	www.tandfonline.com/doi/full/10.1080/09688080.2017.1401893
62	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Programme potential for the prevention of and response to sexual violence among female refugees a literature review	Gianna Maxi Leila Robbers, Alison Morgan	2017	Nee	Nee	tandfonline	2 keer gevonden als resultaat in zelfde zoekmachine	www.tandfonline.com/doi/full/10.1080/09688080.2017.1401893
63	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Service Quality in Software-as-a-Service: Developing the SaaS-Qual Measure and Examining Its Role in Usage Continuance	Alexander Benlian, Marios Koufaris, Thomas Hess	2012	Nee	X	Erasmus bibliotheek	Link werkt niet, niet te vinden op Erasmus bibliotheek	

#	Relevantie DV	Datum	Zoekbron	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
64	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams	Michael E Edge, Pedro R Falcone Sampaio	2012	Nee	X	sciencedirect	Zelfde artikel als 55	www.sciencedirect.com/science/article/pii/S0957417412001637
65	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Care zoning. A pragmatic approach to enhance the understanding of clinical needs as it relates to clinical risks in acute in-patient unit settings.	Taylor K, Guy S, Stewart L, Ayling M, Miller G, Anthony A, Bajuk A, Brun JL, Shearer D, Gregory R, Thomas M	2011	Nee	Nee		Medisch	www.tandfonline.com/doi/full/10.3109/01612840.2011.559570
66	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	In This Issue	Geen naam genoemd	2013	Nee	Nee	jstor	Medisch	www.sciencedirect.com/science/article/pii/S0085253815301484
67	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	POSTER PRESENTATIONS	Panattoni G; Papavasileiou LP; Della Rocca	2011	Nee	NEe	wiley	Medisch	www.sciencedirect.com/science/article/pii/S0020729215300047
68	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Factors affecting recruitment and retention of community health workers in a newborn care intervention in Bangladesh	Syed Rahman, Nabeel Ali, Larissa Jennings, M Habibur R Seraji, Ishtiaq Mannan, Rasheduzzaman Shah, Arif Al-Mahmud, Sanwarul Bari, Daniel Hossain, Milan Das, Abdullah H Baqui, Shams El Arifeen, Peter J Winch	2010	Nee	Nee	ncbi	Medisch	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1478-4491%5Bjour%5D+AND+8%5Bvolume%5D+AND+12%5Bpage%5D+AND+2010%5Bpdat%5D
69	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Factors affecting recruitment and retention of community health workers in a newborn care intervention in Bangladesh	Syed Rahman, Nabeel Ali, Larissa Jennings, M Habibur R Seraji, Ishtiaq Mannan, Rasheduzzaman Shah, Arif Al-Mahmud, Sanwarul Bari, Daniel Hossain, Milan Das, Abdullah H Baqui, Shams El Arifeen, Peter J Winch	2010	Nee	Nee	ncbi	Medisch, 4 keer gevonden als resultaat in zelfde zoekmachine	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1478-4491%5Bjour%5D+AND+8%5Bvolume%5D+AND+12%5Bpage%5D+AND+2010%5Bpdat%5D
70	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	The importance of Malaysian Land Administration Domain Model country profile in land policy	Nur Amalina Zulkifli, Alias Abdul Rahman, Peter van Oosterom, Liat Choon Tan, Hasan Jamil, Chee Hua Teng, Kam Seng Looi, Keat Lim Chan	2015	Nee	Nee	sciencedirect		www.sciencedirect.com/science/article/pii/S0264837715002240
71	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Factors affecting recruitment and retention of community health workers in a newborn care intervention in Bangladesh	Syed Rahman, Nabeel Ali, Larissa Jennings, M Habibur R Seraji, Ishtiaq Mannan, Rasheduzzaman Shah, Arif Al-Mahmud, Sanwarul Bari, Daniel Hossain, Milan Das, Abdullah H Baqui, Shams El Arifeen, Peter J Winch	2010	Nee	Nee	ncbi	Medisch, 4 keer gevonden als resultaat in zelfde zoekmachine	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1478-4491%5Bjour%5D+AND+8%5Bvolume%5D+AND+12%5Bpage%5D+AND+2010%5Bpdat%5D
72	DV 2	31/07/2019	Erasmus bibliotheek	Systematisch	Information Security Framework(s) AND Continuous Delivery	Samenvatting + sinds 2010, Peer-Reviewed, Engels	Factors affecting recruitment and retention of community health workers in a newborn care intervention in Bangladesh	Syed Rahman, Nabeel Ali, Larissa Jennings, M Habibur R Seraji, Ishtiaq Mannan, Rasheduzzaman Shah, Arif Al-Mahmud, Sanwarul Bari, Daniel Hossain, Milan Das, Abdullah H Baqui, Shams El Arifeen, Peter J Winch	2010	Nee	Nee	ncbi	Medisch, 4 keer gevonden als resultaat in zelfde zoekmachine	www.ncbi.nlm.nih.gov/pmc/?cmd=Search&term=1478-4491%5Bjour%5D+AND+8%5Bvolume%5D+AND+12%5Bpage%5D+AND+2010%5Bpdat%5D
73	DV 2			Aangereikt door begeleider	nvt		The Revival of Ancient Information Security Models, Insight in Risks and Selection of Measures	S Schinagl, R Paans, K Schoon	2016	Ja	Ja	Researchgate	Aangereikt door begeleider PhD Y. Bobbert	www.researchgate.net/profile/Ronald_Paans/publication/300409231_The_Revival_of_Ancient_Information_Security_Models_Insight_in_Risks_and_Selection_of_Measures/links/59ec9ce64585151983cccf6b/The-Revival-of-Ancient-Information-Security-Models-Insight-in-Risks-and-Selection-of-Measures.pdf

Bijlage 1.3 - Zoekresultaten deelvraag 3

#	Relevant voor?	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
1	DV 3	Google Scholar	31/07/2019	Systematisch	Security Continuous Deployment Pipeline	Titel, sinds 2010	Security Support in Continuous Deployment Pipeline	Faheem Ullah, Adam Johannes Raft, Mojtaba Shahin, Mansooreh Zahedi, Muhammad Ali Babar	2017	Ja	Ja	arxiv		arxiv.org/abs/1703.04277
2	DV 3	Google Scholar	31/07/2019	Systematisch	Security Continuous Delivery	Titel, sinds 2010	Automated Cloud Infrastructure, Continuous Integration and Continuous Delivery using Docker with Robust Container Security	S Garg, S Garg	2019	Ja	Nee	computer.org, IEEE Computer Society	Betaalde artikel, gevonden via erasmus bibliotheek	ieeexplore.ieee.org/abstract/document/8695332
3	DV 3	Google Scholar	31/07/2019	Systematisch	Security Continuous Delivery	Titel, sinds 2010	A framework for detecting and preventing security vulnerabilities in continuous integration/continuous delivery pipelines	M Koopman	2019	Ja	Ja	utwente		essay.utwente.nl/78048/
4	DV 3	Google Scholar	31/07/2019	Systematisch	Information Security measures AND Cloud	Titel, sinds 2010	Towards quantitative measures of Information Security: A Cloud Computing case study	M Jouini, AB Aissa, LBA Rabai	2012	Ja	Nee	Researchgate		www.researchgate.net/profile/Anis_Aissa/publication/235770867_Towards_quantitative_measures_of_Information_Security_A_Cloud_Computing_case_study/links/09e4151366591c80a5000000/Towards-quantitative-measures-of-Information-Security-A-Cloud-Computing-case-study.pdf
5	DV 3	Google Scholar	31/07/2019	Systematisch	Information Security measures AND Cloud	Titel, sinds 2010	Information security risk measures for Cloud-based Personal Health Records	A Mxoli, M Gerber	2014	Nee	Nee	IEEE Xplore		ieeexplore.ieee.org/abstract/document/7009039
6	DV 3	Google Scholar	31/07/2019	Systematisch	Information Security measures AND Cloud	Titel, sinds 2010	The Impact of Information Security Measures Analysis of Cloud Computing	K Xing-bin Song Yuan-yuan	2011	Ja	X	cnki	Kom op een aziatisch site terecht	en.cnki.com.cn/Article_en/CJFDTotal-AQJS201110009.htm
7	DV 3	Google Scholar	31/07/2019	Systematisch	Information Security measures AND Cloud	Titel, sinds 2010	Review on Cryptographic Measures for Information Security in Cloud	D Santhadevi, A Chhabra	2014	Nee	Nee	indianjournals		www.indianjournals.com/ijor.aspx?target=ijor:iitmjmit&volume=5&issue=1&article=011
8	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Deployment Pipelines	Titel	Practical deployment of pipelines for the CCS network in critical conditions using MINLP modelling and optimization: A case study of South Korea	Changsoo Kim, Kyeongsu Kim, Jeongnam Kim, Usama Ahmed, Chonghun Han	2018	Nee	Nee	Science Direct		www.sciencedirect.com/science/article/pii/S1750583617306886
9	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Continuous Delivery	Titel, sinds 2010, Peer-Reviewed	Continuous measurement of cardiac output with the electrical velocimetry method in patients under spinal anesthesia for cesarean delivery	Yanhong Liu, May C M Pian-Smith, Lisa R Leffert, Rebecca D Minehart, Andrea Torri, Charles Coté, Robert M Kacmarek, Yandong Jiang	2015	Nee	Nee	Springer		link.springer.com/article/10.1007%2Fs10877-014-9645-8
10	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Security Measures AND Continuous Deployment Pipeline	Samenvatting, sinds 2010, Peer-Reviewed	REPORT OF THE FINANCE AND TRANSACTIONS COMMITTEE	Anonymous	2018	Nee	Nee	heinonline		heinonline.org/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/energy35&men_hide=false&men_tab=toc&kind=&page=1
11	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Deployment Pipelines	Samenvatting, sinds 2010, Peer-Reviewed	Regulated software meets DevOps	Teemu Laukkarinen, Kati Kuusinen, Tommi Mikkonen	2018	Nee	Nee	Elsevier ScienceDirect		www.sciencedirect.com/science/article/pii/S0950584918300144
12	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Deployment Pipelines	Samenvatting, sinds 2010, Peer-Reviewed	Table stakes for modern software development	Mark Ferlatte, Nic Wissman	2018	Nee	Nee	ProQuest		search.proquest.com/docview/2136875291
13	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Security Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Cloud based E-Learning, Security Threats and Security Measures	Umar Shoaib, Ghulam Abbas, Muhammad Atif Sattar	2016	Ja	Nee	indjst	2 keer gevonden als resultaat in zelfde zoekmachine	www.indjst.org/index.php/indjst/article/download/96166/77340
14	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Cloud Computing in the Global South: drivers, effects and policy measures	NIR KSHETRI	2011	Nee	Nee	tandfonline	2 keer gevonden als resultaat in zelfde zoekmachine	www.tandfonline.com/doi/full/10.1080/01436597.2011.586225
15	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Analysis of performance measures in cloud-based ubiquitous SaaS CRM project systems	You-Shyang Chen, Chienwen Wu, Heng-Hsing Chu, Chien-Ku Lin, Huan-Ming Chuang	2018	Nee	Nee	Springer		link.springer.com/search?dc.title=Analysis+of+performance+measures+in+cloud-based+ubiquitous+SaaS+CRM+project+systems.&date-facet-mode=between&facet-start-year=2018&dc.creator=chen&showAll=true
16	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Risk Involved in Cloud Data Storage and its Safety Measures	K Mythili, S Rajalakshmi	2014	Nee	Nee	ijcaonline		www.ijcaonline.org/
17	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Full-waveform LiDAR point cloud land cover classification with volumetric texture measures	Tsai F, Lai J-S, Lu Y-H	2016	Nee	Nee	cgu		tao.cgu.org.tw/index.php/articles/archive/space-science/item/1433
18	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Analysis of performance measures in cloud-based ubiquitous SaaS CRM project systems.	Y S Chen, C Wu, H H Chu, C K Lin	2018	Nee	Nee	Springer		link.springer.com/search?dc.title=Analysis+of+performance+measures+in+cloud-based+ubiquitous+SaaS+CRM+project+systems.&date-facet-mode=between&facet-start-year=2018&dc.creator=chen&showAll=true
19	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Cloud computing for small business: Criminal and security threats and prevention measures	Hutchings A, Smith RG, James L	2013	Nee	Nee	aic		www.aic.gov.au/publications/current%20series/tandi.aspx
20	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Novel security issues and mitigation measures in cloud computing: an Indian perspective	Sudhakar Godi	2018	Ja	X	Erasmus bibliotheek	Betaalde artikel, NIET gevonden via erasmus bibliotheek	search.proquest.com/docview/2130408031/fulltext/

#	Relevant voor?	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
21	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Touring the atmosphere aboard the A-Train A convoy of satellites orbiting Earth measures cloud properties, greenhouse gas concentrations, and more to provide a multifaceted perspective on the processes that affect climate	Tristan S L'Ecuyer, Jonathan H Jiang	2010	Nee	Nee	Erasmus bibliotheek	2 keer gevonden als resultaat in zelfde zoekmachine	eur.on.worldcat.org/search?databaseList=10052%2C2198%2C2274%2C3561%2C1060%2C2229%2C1931%2C3837%2C233%2C1697%2C2269%2C1653%2C2268%2C3313%2C3036%2C2662%2C239%2C3950%2C638%2C2507%2C1978%2C3834%2C10060%2C4069%2C3374%2C1271%2C2314%2C2358%2C2237%2C2236%2C2038%2C1982%2C203%2C3841%2C3967%2C2375%2C2572%2C2175%2C3384%2C2294%2C3382%2C1082%2C3538%2C1910%2C2369%2C3018%2C2006%2C3577%2C2443%2C3652%2C3976%2C2462%2C2264%2C2263%2C2261%2C2260%2C3195%2C143%2C1842%2C2215%2C2897%2C2259%2C3589%2C983%2C3225%2C1609%2C10046%2C946%2C3986%2C1847%2C3988&queryString=ti%3A+Touring+the+atmosphere+aboard+the+A-Train+A+convoy+of+satellites+orbiting+Earth+measures+cloud+properties%2C+greenhouse+gas+concentrations%2C+and+more+to+provide+a+multifaceted+perspective+on+the+processes+that+affect+climate&clusterResults=true#/oclc/4885267404
22	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Combining reputation and QoS measures to improve cloud service composition	Fabrizio Messina, Giuseppe Pappalardo, Antonello Comi, Lidia Fotia, Giuseppe ML Sarné, Domenico Rosaci	2017	Nee	Nee	Erasmus bibliotheek		eur.on.worldcat.org/search?databaseList=10052%2C2198%2C2274%2C3561%2C1060%2C2229%2C1931%2C3837%2C233%2C1697%2C2269%2C1653%2C2268%2C3313%2C3036%2C2662%2C239%2C3950%2C638%2C2507%2C1978%2C3834%2C10060%2C4069%2C3374%2C1271%2C2314%2C2358%2C2237%2C2236%2C2038%2C1982%2C203%2C3841%2C3967%2C2375%2C2572%2C2175%2C3384%2C2294%2C3382%2C1082%2C3538%2C1910%2C2369%2C3018%2C2006%2C3577%2C2443%2C3652%2C3976%2C2462%2C2264%2C2263%2C2261%2C2260%2C3195%2C143%2C1842%2C2215%2C2897%2C2259%2C3589%2C983%2C3225%2C1609%2C10046%2C946%2C3986%2C1847%2C3988&queryString=ti%3A+Combining+reputation+and+QoS+measures+to+improve+cloud+service+composition&clusterResults=true#/oclc/7126308320
23	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Cloud service reliability assessment approach based on multi-valued neutrosophic cross-entropy and entropy measures	Wang Y, Wang X-K, Wang J-Q	2018	Nee	Nee	Erasmus bibliotheek		eur.on.worldcat.org/search?databaseList=10052%2C2198%2C2274%2C3561%2C1060%2C2229%2C1931%2C3837%2C233%2C1697%2C2269%2C1653%2C2268%2C3313%2C3036%2C2662%2C239%2C3950%2C638%2C2507%2C1978%2C3834%2C10060%2C4069%2C3374%2C1271%2C2314%2C2358%2C2237%2C2236%2C2038%2C1982%2C203%2C3841%2C3967%2C2375%2C2572%2C2175%2C3384%2C2294%2C3382%2C1082%2C3538%2C1910%2C2369%2C3018%2C2006%2C3577%2C2443%2C3652%2C3976%2C2462%2C2264%2C2263%2C2261%2C2260%2C3195%2C143%2C1842%2C2215%2C2897%2C2259%2C3589%2C983%2C3225%2C1609%2C10046%2C946%2C3986%2C1847%2C3988&queryString=ti%3A+Cloud+service+reliability+assessment+approach+based+on+multi-valued+neutrosophic+cross-entropy+and+entropy+measures&clusterResults=true#/oclc/8012271524
24	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Classifying and Filtering Users by Similarity Measures for Trust Management in Cloud Environment	Fatima Zohra Filali, Belabbas Yagoubi	2015	Nee	Nee	scpe		www.scpe.org/index.php/scpe/article/download/1102/443
25	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	A Proposition of Modifications and Extensions of Cloud Computing Standards for Trust Characteristics Measures	Sara Moazzezi Eftekhar, Witold Suryn	2019	Nee	Nee	Erasmus bibliotheek		eur.on.worldcat.org/search?databaseList=10052%2C2198%2C2274%2C3561%2C1060%2C2229%2C1931%2C3837%2C233%2C1697%2C2269%2C1653%2C2268%2C3313%2C3036%2C2662%2C239%2C3950%2C638%2C2507%2C1978%2C3834%2C10060%2C4069%2C3374%2C1271%2C2314%2C2358%2C2237%2C2236%2C2038%2C1982%2C203%2C3841%2C3967%2C2375%2C2572%2C2175%2C3384%2C2294%2C3382%2C1082%2C3538%2C1910%2C2369%2C3018%2C2006%2C3577%2C2443%2C3652%2C3976%2C2462%2C2264%2C2263%2C2261%2C2260%2C3195%2C143%2C1842%2C2215%2C2897%2C2259%2C3589%2C983%2C3225%2C1609%2C10046%2C946%2C3986%2C1847%2C3988&queryString=ti%3A+A+Proposition+of+Modifications+and+Extensions+of+Cloud+Computing+Standards+for+Trust+Characteristics+Measures&clusterResults=true#/oclc/8186244046
26	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Analysis of performance measures to improve the quality of service in cloud based e-government web portal	Priya V, Subha S, Balamurugan B	2018	Nee	Nee	inderscience		www.inderscience.com/storage/f691547111210382.pdf

#	Relevant voor?	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
27	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Measures AND Cloud	Titel, sinds 2010, Peer-Reviewed	Amplifying Spatial Awareness via GIS: Tech which brings Healthcare Management, Preventative & Predictive Measures under the same Cloud	Este Geraghty	2015	Nee	Nee	Erasmus bibliotheek		eur.on.worldcat.org/search?databaseList=10052%2C2198%2C2274%2C3561%2C1060%2C2229%2C1931%2C3837%2C233%2C1697%2C2269%2C1653%2C2268%2C3313%2C3036%2C2662%2C239%2C3950%2C638%2C2507%2C1978%2C3834%2C10060%2C4069%2C3374%2C1271%2C2314%2C2358%2C2237%2C2236%2C2038%2C1982%2C203%2C3841%2C3967%2C2375%2C2572%2C2175%2C3384%2C2294%2C3382%2C1082%2C3538%2C1910%2C2369%2C3018%2C2006%2C3577%2C2443%2C3652%2C3976%2C2462%2C2264%2C2263%2C2261%2C2260%2C3195%2C143%2C1842%2C2215%2C2897%2C2259%2C3589%2C983%2C3225%2C1609%2C10046%2C946%2C3986%2C1847%2C3988&queryString=ti%3A+Amplifying+Spatial+Awareness+via+GIS%3A+Tech+which+brings+Healthcare+Management%2C+Preventative+%26+Predictive+Measures+under+the+same+Cloud#/oclc/5913383723
28	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Analysis of recommended cloud security controls to validate OpenPMF "policy as a service"	Ulrich Lang, Rudolf Schreiner	2011	Ja	Ja	Elsevier ScienceDirect	Ook relevant voor DV 4	www.sciencedirect.com/science/article/pii/S136341271100046X
29	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Cross-layer-based adaptive congestion and contention controls for accessing cloud services in 5G IEEE 802.11 family wireless networks	Ben-Jye Chang, Shin-Pin Chen	2017	Nee	Nee	Elsevier ScienceDirect		www.sciencedirect.com/science/article/pii/S0140366417302517
30	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Who controls the cloud?	RE Leenes	2010	Nee	Nee	DOAJ		doaj.org/search?source=%7B%22query%22%3A%7B%22query_string%22%3A%7B%22query%22%3A%22Who%5C%5C%2Bcontrols%5C%5C%2Bthe%5C%5C%2Bcloud%5C%5C%3F%22%2C%22default_field%22%3A%22bibjson.title%22%2C%22default_operator%22%3A%22AND%22%7D%7D%2C%22from%22%3A0%2C%22size%22%3A10%7D
31	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	CLOUD COMPUTING, EXPORT CONTROLS, AND SANCTIONS	Richard Tauwhare	2015	Ja	Nee	ProQuest		search.proquest.com/docview/1705536921
32	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Trust in cloud services: Providing more controls to clients	Khan KM, Malluhi Q	2013	Nee	Nee	IEEE Xplore		www.computer.org/csdl/magazine/co/2013/07
33	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Clicking the "Export" Button: Cloud Data Storage and U.S. Dual-Use Export Controls.	Joseph A Schoorl	2012	Nee	Nee	heinonline		heinonline.org/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/gwlr80&men_hide=false&men_tab=toc&kind=&page=632
34	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Springtime cloud properties in the Taiwan Strait: synoptic controls and local processes	Mien-Tze Kueh, Pay-Liam Lin	2014	Nee	Nee	Springer		link.springer.com/article/10.1007%2Fs00704-013-0969-y
35	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Formal modeling and verification of security controls for multimedia systems in the cloud.	M Alam	2017	Ja	Nee	Springer	5 keer gevonden als resultaat in zelfde zoekmachine	link.springer.com/search?dc.title=Formal+modeling+and+verification+of+security+controls+for+multimedia+systems+in+the+cloud.&date-facet-mode=between&facet-start-year=2017&dc.creator=alam&showAll=true
36	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Influence of Below-Cloud Evaporation on Deuterium Excess in Precipitation of Arid Central Asia and Its Meteorological Controls	Shengjie Wang, Mingjun Zhang, Yanjun Che, Xiaofan Zhu, Xuemei Liu	2016	Nee	Nee	American Meteorological Society		journals.ametsoc.org/action/doSearch?type=advanced&displaySummary=true&author=wang&title=Influence+of+Below-Cloud+Evaporation+on+Deuterium+Excess+in+Precipitation+of+Arid+Central+Asia+and+Its+Meteorological+Controls&searchText=&abstract=&pubidspan=&categoryId=40000013&filter=multiple&start=&end=&Search=Search&
37	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	IT controls in the public cloud: Success factors for allocation of roles and responsibilities	Khan S, Nicho M, Takruri H	2016	Ja	X	ProQuest	Betaalde artikel, niet verkrijgbaar via erasmus bibliotheek	eur.on.worldcat.org/search?databaseList=10052%2C2198%2C2274%2C3561%2C1060%2C2229%2C1931%2C3837%2C233%2C1697%2C2269%2C1653%2C2268%2C3313%2C3036%2C2662%2C239%2C3950%2C638%2C2507%2C1978%2C3834%2C10060%2C4069%2C3374%2C1271%2C2314%2C2358%2C2237%2C2236%2C2038%2C1982%2C203%2C3841%2C3967%2C2375%2C2572%2C2175%2C3384%2C2294%2C3382%2C1082%2C3538%2C1910%2C2369%2C3018%2C2006%2C3577%2C2443%2C3652%2C3976%2C2462%2C2264%2C2263%2C2261%2C2260%2C3195%2C143%2C1842%2C2215%2C2897%2C2259%2C3589%2C983%2C3225%2C1609%2C10046%2C946%2C3986%2C1847%2C3988&queryString=ti%3A+IT+controls+in+the+public+cloud%3A+Success+factors+for+allocation+of+roles+and+responsibilities&clusterResults=true#/oclc/1064077599

#	Relevant voor?	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
38	DV 3	Erasmus Bibliotheek	31/07/2019	Systematisch	Controls AND Cloud	Titel, sinds 2010, Peer-Reviewed	Intercrossed access controls for secure financial services on multimedia big data in cloud systems	Li Y, Gai K, Qiu M, Ming Z, Zhao H	2016	Nee	X	Erasmus bibliotheek	Betaalde artikel, niet verkrijgbaar via erasmus bibliotheek	eur.on.worldcat.org/search?databaseList=10052%2C2198%2C2274%2C3561%2C1060%2C2229%2C1931%2C3837%2C233%2C1697%2C2269%2C1653%2C2268%2C3313%2C3036%2C2662%2C239%2C3950%2C638%2C2507%2C1978%2C3834%2C10060%2C4069%2C3374%2C1271%2C2314%2C2358%2C2237%2C2236%2C2038%2C1982%2C203%2C3841%2C3967%2C2375%2C2572%2C2175%2C3384%2C2294%2C3382%2C1082%2C3538%2C1910%2C2369%2C3018%2C2006%2C3577%2C2443%2C3652%2C3976%2C2462%2C2264%2C2263%2C2261%2C2260%2C3195%2C143%2C1842%2C2215%2C2897%2C2259%2C3589%2C983%2C3225%2C1609%2C10046%2C946%2C3986%2C1847%2C3988&queryString=ti%3A+Intercrossed+access+controls+for+secure+financial+services+on+multimedia+big+data+in+cloud+systems&clusterResults=true#/oclc/6851989103
39	DV 3	Erasmus Bibliotheek	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	Securing a Deployment Pipeline	Bass, L; Holz, R; Rimba, P; Tran, AB; Zhu, L	2015	Ja	Ja	UNSWork	Via artikel van Koopman (2019)	www.unsworks.unsw.edu.au/primo-explore/fulldisplay?vid=UNSWORKS&docid=unsworks_modsunsworks_13700&context=L
40	DV 3	Erasmus Bibliotheek	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	Security Requirements Engineering in the Agile Era: How Does it Work in Practice?	M Daneva, C Wang	2018	Ja	Nee	computer.org, IEEE Computer Society	Via artikel van Koopman (2019)	www.computer.org/csdl/proceedings-article/2018/quarap/17D45VtKiqz/17D45VUZMVT
41	DV 3	Erasmus Bibliotheek	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	Continuous deployment of software intensive products and services: A systematic mapping study	Pilar Rodríguez, Alireza Haghighatkhah, Lucy Ellen Lwakatare, Susanna Teppola, Tanja Suomalainen, Juho Eskeli, Teemu Karvonen, Pasi Kuvaja, June M Verner, Markku Oivo	2017	Nee	Nee	Science Direct	Via artikel van Koopman (2019)	www.sciencedirect.com/science/article/pii/S0164121215002812
42	DV 3	Erasmus Bibliotheek	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	Continuous Integration, Delivery and Deployment: A Systematic Review on Approaches, Tools, Challenges and Practices	Mojtaba Shahin, Muhammad Ali Babar, Liming Zhu	2017	Nee	Nee	IEEE Xplore	Via artikel van Koopman (2019)	ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7884954
43	DV 3	Erasmus Bibliotheek	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	A Systematic Mapping Study on Security in Agile Requirements Engineering	Hugo Villamizar, Marcos Kalinowski, Marx Viana, Daniel Méndez Fernández	2018	Ja	Nee	computer.org, IEEE Computer Society	Via artikel van Koopman (2019)	www.computer.org/csdl/proceedings-article/2018/seaa/17D45VtKiqd/17D45WHONht
44	DV 3	Google Scholar	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	Security of Public Continuous Integration Services	V Gruhn, C Hannebauer, C John	2013	Ja	Nee	psu.edu	via artikel van Mojtaba Shahin, Muhammad Ali Babar, Liming Zhu (2017)	citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.739.5458&rep=rep1&type=pdf
45	DV 3	Google Scholar	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	What is devops?: A systematic mapping study on definitions and practices	R Jabbari, N bin Ali, K Petersen	2016	Nee	Nee	Researchgate	Via artikel van Koopman (2019), geen focus op security	www.researchgate.net/profile/Ramtin_Jabbari/publication/308857081_What_is_DevOps_A_Systematic_Mapping_Study_on_Definitions_and_Practices/links/5aa2ae9145851543e63c223a/What-is-DevOps-A-Systematic-Mapping-Study-on-Definitions-and-Practices.pdf
46	DV 3	Google Scholar	31/07/2019	Sneeuwbal methode	Volledige titel	Titel	Trade-Offs in Continuous Integration: Assurance, Security, and Flexibility	M Hilton, N Nelson, T Tunnell, D Marinov	2017	Ja	Nee	oregonstate	Via artikel van Koopman (2019)	web.engr.oregonstate.edu/~nelsonni/docs/fse17-hilton.pdf

Bijlage 1.4 - Zoekresultaten deelvraag 4

#	Relevant voor?	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
1	DV 4	Google Scholar	31/07/2019	Systematisch	Information Security Measures AND Automation	Titel, sinds 2010	Protection of Intellectual Property of the Plant Continuity through IT/OT Cyber Security Measures and Governance into Industrial Automation & Control Systems	A Mason	2018	Nee	Nee	ProQuest		search.proquest.com/openview/0a2bf646ba3ed0d426a5a89138e4ef18/1?pq-origsite=gscholar&cbl=18750&diss=y
2	DV 4	Google Scholar	31/07/2019	Systematisch	Information Security Measures AND Automated	Titel, sinds 2010	Security measures in automated assessment system for programming courses	J Šťastná, J Juhár, M Biňas, M Tomášek	2015	Nee	Nee	vse		www.ceeol.com/search/article-detail?id=663688
3	DV 4	Google Scholar	31/07/2019	Systematisch	Information Security Measures AND Automated	Titel, sinds 2010	Evaluation Of Current Security Measures Used In Automated Teller Machines (ATM)	K Setlalekgosi	2019	Nee	Nee	sunderland		sure.sunderland.ac.uk/id/eprint/10822/1/Selected%20Computing%20Research%20Papers%20June%202019.pdf#page=51
4	DV 4	Google Scholar	31/07/2019	Systematisch	Information Security Controls AND Automated	Titel, sinds 2010	Information Security Controls against Cross-Site Request Forgery Attacks on Software Applications of Automated Systems	AV Barabanov, AS Markov	2018	Ja	Nee	iop	6 keer gevonden als resultaat in zelfde zoekmachine	iopscience.iop.org/article/10.1088/1742-6596/1015/4/042034/meta
5	DV 4	Google Scholar	31/07/2019	Systematisch	Security Controls AND Automation	Titel, sinds 2010	SIEM-based framework for security controls automation	R Montesino, S Fenz, W Baluja	2012	Ja	Ja	emerald	6 keer gevonden als resultaat in zelfde zoekmachine	www.emerald.com/insight/content/doi/10.1108/09685221211267639/full/html
6	DV 4	Google Scholar	31/07/2019	Systematisch	Security Controls AND Automated	Titel, sinds 2010	Automated audit of compliance and security controls	G Koschorreck	2011	Ja	Nee	IEEE Xplore computer.org		ieeexplore.ieee.org/abstract/document/5931118
7	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Deployment Pipeline	Titel, sinds 2010	Automated Verification of Load Test Results in a Continuous Delivery Deployment Pipeline	N Sundbaum	2015	Nee	Nee	Digitala Vetenskapliga Arkivet	2 keer gevonden als resultaat in zelfde zoekmachine	www.diva-portal.org/smash/record.jsf?pid=diva2%3A824273&dswid=topdog
8	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Deployment Pipeline	Titel, sinds 2010	Automated Key Rotations In a Continuous Deployment Pipeline	J Rylander, J Moberg	2018	Ja	Ja	Digitala Vetenskapliga Arkivet		www.diva-portal.org/smash/record.jsf?pid=diva2%3A1230071&dswid=topdog
9	DV 4	Google Scholar	31/07/2019	Systematisch	Automation AND Continuous Delivery	Titel, sinds 2010	Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation	J Humble, D Farley	2010	Ja	Nee	pearson	Boek	
10	DV 4	Google Scholar	31/07/2019	Systematisch	Automation AND Continuous Delivery	Titel, sinds 2010	End to end automation on cloud with build pipeline: the case for DevOps in insurance industry, continuous integration, continuous testing, and continuous delivery	M Soni	2015	Ja	Nee	IEEE Xplore computer.org		ieeexplore.ieee.org/abstract/document/7436936
11	DV 4	Google Scholar	31/07/2019	Systematisch	Automation AND Continuous Delivery	Titel, sinds 2010	Continuous Integration and Continuous Delivery Pipeline Automation for Agile Software Project Management	S Arachchi, I Perera	2018	Ja	X	IEEE Xplore computer.org	Betaalde artikel, niet gevonden via erasmus bibliotheek	ieeexplore.ieee.org/abstract/document/8421965
12	DV 4	Google Scholar	31/07/2019	Systematisch	Automation AND Continuous Delivery	Titel, sinds 2010	Towards continuous delivery in system integration projects: introducing a strategy to achieve continuous delivery and test automation with FitNesse	S Drenthen	2014	Ja	Nee	utwente		essay.utwente.nl/64984/
13	DV 4	Google Scholar	31/07/2019	Systematisch	Automation AND Continuous Delivery	Titel, sinds 2010	Reactor automation in continuous flow polymerisation: on-demand delivery of precision polymer materials	JJ Haven, T Junkers	2018	Nee	Nee	uhdspace		uhdspace.uhasselt.be/dspace/handle/1942/27556
14	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Delivery	Titel, sinds 2010	Automated testing in the continuous delivery pipeline: A case study of an online company	J Gmeiner, R Ramler, J Haslinger	2015	Ja	Nee	IEEE Xplore computer.org		ieeexplore.ieee.org/abstract/document/7107423
15	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Delivery	Titel, sinds 2010	Automated regression testing of BPMN 2.0 processes: a capture and replay framework for continuous delivery	M Makki, D Van Landuyt, W Joosen	2016	Nee	Nee	acm	Betaalde artikel, niet gevonden via erasmus bibliotheek	dl.acm.org/citation.cfm?id=2993257
16	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Delivery	Titel, sinds 2010	Automated Testing for Continuous Delivery Pipelines	Justin Wolf, Scott Yoon	2016	Ja	Nee	pnsqc		uploads.pnsqc.org/2016/papers/13.AutomatedTestingForContinuousDeliveryPipelines.pdf
17	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Delivery	Titel, sinds 2010	Automated build service to facilitate Continuous Delivery	T Karlsson	2015	Nee	Nee	lub.lu		lup.lub.lu.se/student-papers/search/publication/7449594
18	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Delivery	Titel, sinds 2010	Automated Cloud Infrastructure, Continuous Integration and Continuous Delivery using Docker with Robust Container Security	S Garg, S Garg	2019	Ja	Nee	computer.org, IEEE Computer Society	Betaalde artikel, gevonden via erasmus bibliotheek	ieeexplore.ieee.org/abstract/document/8695332
19	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Delivery	Titel, sinds 2010	Ultrasound-guided continuous interscalene block: the influence of local anesthetic delivery method (automated bolus versus continuous infusion) on postoperative	M Hamdani, O Chassot, P Hoffmeyer	2013	Nee	Nee	lww		journals.lww.com/ejanaesthesiology/Fulltext/2013/06001/Ultrasound_guided_continuous_interscalene_block_.362.aspx

#	Relevant voor?	Zoekbron	Datum	Zoekmethode	Zoekterm	Zoekkader	Titel artikel	Auteur(s)	Jaar	Relevantie titel	Relevantie content	Gevonden op	Aantekeningen	URL
20	DV 4	Google Scholar	31/07/2019	Systematisch	Automated AND Continuous Delivery	Titel, sinds 2010	Method and Apparatus for the Automated Delivery of Continuous Neural Stem Cell Trails Into the Spinal Cord of Small and Large Animals	AB Kutikov, SW Moore, RT Layer, PE Podell	2018	Nee	Nee	Researchgate		www.researchgate.net/profile/James_Guest2/publication/327318412_Method_and_Apparatus_for_the_Automated_Delivery_of_Continuous_Neural_Stem_Cell_Trails_Into_the_Spinal_Cord_of_Small_and_Large_Animals/links/5b8801cb299bf1d5a732055e/Method-and-Apparatus-for-the-Automated-Delivery-of-Continuous-Neural-Stem-Cell-Trails-Into-the-Spinal-Cord-of-Small-and-Large-Animals.pdf
21	DV 4	Erasmus Bibliotheek	31/07/2019	Systematisch	Information Security Controls AND Automation	Titel, sinds 2010, Peer-Reviewed	Research on Information Security Interaction Mode of Mobile Devices Based on Ubiquitous Computing	Xianquan Zeng	2015	Nee	Nee	Open Access eJournals		www.bentham.org/open/toautocj/
22	DV 4	Erasmus Bibliotheek	31/07/2019	Systematisch	Continuous Delivery AND Automation	Titel, sinds 2010, Peer-Reviewed	Continuous performance monitoring of industrial products as a key to their safe delivery and operation	Yu Buryak	2010	Nee	Nee	Springer		link.springer.com/search?dc.title=Continuous+performance+monitoring+of+industrial+products+as+a+key+to+their+safe+delivery+and+operation.&date-facet-mode=between&facet-start-year=2010&dc.creator=buryak&showAll=true

Bijlage 2 - Voorbereiding participant op het interview

In deze bijlage is de email opgenomen die ter voorbereiding persoonlijk aan de participanten is gestuurd. Het doel van deze email is om het doel van het onderzoek, de definitie van gehanteerde termen en de verwachtingen aan de participanten toe te lichten. Dit omdat ze dan de handvaten krijgen om zichzelf op een gedegen manier voor te bereiden.

Beste (naam participant),

Middels deze email wil ik je uitnodigen om deel te nemen aan mijn Master afstudeeronderzoeksproject. In deze email zal ik het doel van mijn onderzoek nader toelichten als voorbereiding op het interview wat ik met je ga hebben. Deelname aan dit onderzoek is geheel vrijwillig, anoniem en er zal geen (geldelijke) beloning tegenover staan. Je kunt te allen tijde zonder verdere toelichting besluiten om je terug te trekken en niet meer deel te nemen aan dit onderzoek.

Op basis van het proefinterview wat is gehouden met één expert is gebleken dat de voorbereiding op het interview ongeveer twee uur in beslag neemt, het daadwerkelijke interview één uur en de validatie van het interviewverslag een half uur. Dit maakt tezamen een tijdsbesteding van drie en een half uur totaal.

Het doel van dit onderzoek is om te bepalen welke Information Security Measures in een Continuous Deployment Pipeline geautomatiseerd kunnen worden zodat een Continuous Compliance Framework bewerkstelligd kan worden. Hiermee is dit een uniek onderzoeksdomein en jouw hulp daarbij is zeer waardevol voor mij, wetenschap en hopelijk ook jezelf.

Wat verwacht ik van jou?

Ter voorbereiding aan het interview verzoek ik je om de meegeleverde lijst met 131 Information Security Measures door te nemen en bij kolom L en kolom M de juiste antwoorden op basis van jouw expertise in te vullen. Mocht meer informatie nodig zijn over het desbetreffende Topic dan kunnen de filters uitgezet worden om een totaalbeeld te krijgen.

Kolom L: Automatability? Hier kun je aangeven wat je eigen inschatting is op basis van je expertise hoe makkelijk of moeilijk het is om het desbetreffende Topic te automatiseren in een Continuous Deployment Pipeline.

Kolom M: Manual time? Hier kun je aangeven hoeveel tijd het ongeveer zou kosten als je bestaande bewijsmateriaal handmatig zou gaan verzamelen om aan te tonen dat je aan het desbetreffende Topic voldoet. Hierbij kun je ervan uitgaan dat je voldoet aan het topic en dat het bewijsmateriaal bestaat maar nog niet eerder is verzameld.

Graag ontvang ik de ingevulde lijst voor (datum: 3 dagen voor het interview) zodat ik deze vooraf aan het interview kan doornemen. Mocht je enige twijfel of vragen hebben bij het invullen van de lijst dan verzoek ik je om niet een aanname te doen maar contact met mij op te nemen op nummer 0620973948 of neseozkanli@gmail.com Dit om de betrouwbaarheid van mijn onderzoeksresultaat te vergroten.

Onderaan dit mailtje heb ik de definities van de gehanteerde termen toegelicht zodat de meegeleverde lijst op een éénduidige manier wordt geïnterpreteerd en ingevuld.

Nogmaals hartelijk dank en tot (datum van het interview).

Met vriendelijke groet,

Nese Ozkanli

Student Master of Science in Business Process Management & IT aan de Open Universiteit

Gebruikte terminologieën:

Continuous Compliance: "Een continu proces van proactief risicobeheer dat voorspelbare, transparante en kosteneffectieve resultaten oplevert om aan de doelstellingen van informatiebeveiliging te voldoen." (Long, 2015)

Information Security Measures: Literatuuronderzoek heeft gewezen dat de ISF Standard of Good Practice for Information Security (2018) het meest actuele en volledige framework is. Om deze reden is gekozen om de Topics binnen dit framework als Information Security Measures te beschouwen.

Continuous Deployment Pipeline: "Een geautomatiseerd proces om software via een gestructureerd versiebeheer proces (version control) en systeem beschikbaar te maken aan gebruikers. In dit geautomatiseerd proces wordt de software ontwikkeld, in meerdere fases getest en geïmplementeerd op productie" (Humble & Farley, 2010).

Automatisering: "The automatic operation and monitoring of security controls by existing hard – and software security tools, reducing human intervention to a minimum. A security control can be automated if the operation of the control requires only machine-readable and – processable resources (for example, controls such as awareness and security training cannot be automated because they require the training of humans)" (Montesino et al., 2012)

Bijlage 3 - Interview protocol

In deze bijlage is het interview protocol opgenomen dat als leidraad is gebruikt bij het afnemen van de interviews.

Introductie

Voordat het interview start wordt er eerst een introductie gegeven door de interviewer waarin de volgende punten benoemd worden;

- Bedank de participant voor deelnemen en het voorbereiden van het interview
- Kort ingaan van nut en noodzaak van dit onderzoek (praktijk validatie door experten) en je deliverable
- Doel van het interview toelichten
- Toelichten dat de verwerking van het interview anoniem zal zijn en dat de naam van de participant nergens genoemd zal worden
- Toelichten mogelijkheid om niet te antwoorden en te stoppen met het interview
- Toestemming om een audio opname te maken van het interview zodat dit alleen gebruikt kan worden voor de transcriptie. Toelichten dat de audio opname niet met derden wordt gedeeld.
- Toelichting dat participant binnen enkele dagen de uitwerking van het interview krijgt waarop hij/zij kan reageren voordat de gegevens verwerkt worden
- Toestemming om het interview te starten
- Toelichten dat men achteraf de resultaten terugontvangt als het gehele onderzoek is afgerond.

Interviewvragen

1. Wat is jouw definitie van Continuous Compliance?
    a. Wat is een bruikbaar framework voor Continuous Compliance?
    b. Waar zal een Continuous Compliance Framework aan bijdragen?

2. Welke Information Security Frameworks worden veelal gebruikt binnen een Continuous Deployment Pipeline?
    a. Wordt er binnen jouw bedrijf een bepaalde framework gebruikt in de Deployment Pipelines?
        i. Zo ja, welke en waarom vind je dit een geschikt framework?
        ii. Zo nee, heb je een voorkeur voor een bepaalde framework en waarom?

3. Welke Information Security Measures kunnen gesteld worden aan een Continuous Deployment Pipeline?
    a. Wat voor soort Measures kunnen in een Pipeline geautomatiseerd worden en waarom?

4. Welke Information Security Measures kunnen eenvoudig geautomatiseerd worden in een Continuous Deployment Pipeline?
    a. Welke criteria heb je gehanteerd om te kunnen bepalen of de Information Security Measures eenvoudig te automatiseren zijn?
    b. Zijn er binnen jouw bedrijf Information Security Measures geautomatiseerd in een Pipeline?
        i. Zo ja, welke Information Security Measures zijn geautomatiseerd?
    c. Vind je dat waar mogelijk alle Information Security Measures geautomatiseerd moeten worden en waarom?

d. Vind je het ISF framework een goed vertrekpunt om de Information Security Measures te automatiseren en waarom?

Afronding

- Stoppen van de audio opname
- Bedanken voor het interview

Bijlage 4 - Automatable Information Security Measures

			Automatability?														Manual time?											
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
1	Access Control Mechanisms - Password	Principle: Target environments (e.g. business applications, systems or network devices) that are configured with access control mechanisms based on passwords, should require users to provide a valid User ID and password before they can gain access to them. Objective: To prevent unauthorised users from gaining access to password-protected critical or sensitive information, business applications, information systems, networks or computing devices.	Easy	2	Very easy	1	Very easy	1	Easy	2	Neither	3	Easy	2	1,8	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	4,8
2	Business Application Register	Principle: Business applications should be recorded in an accurate and up-to-date business application register. Objective: To record important information about business applications that can be used to support information risk assessments, compare relative risks between applications and identify unauthorised applications.	Very easy	1	Easy	2	Very easy	1	Easy	2	Easy	2	Difficult	4	2,0	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,3
3	Installation Process	Principle: New systems should be installed in the live environment in accordance with a documented installation process. Objective: To minimise disruption to the organisation when new systems are installed in the live environment.	Very easy	1	Easy	2	Easy	2	Easy	2	Neither	3	Easy	2	2,0	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,5
4	Change Management	Principle: Changes to business applications, information systems and network devices should be tested, reviewed and applied using a change management process. Objective: To ensure that changes are applied correctly and do not compromise the security of business applications, computer systems or networks.	Easy	2	Neither	3	Very easy	1	Easy	2	Neither	3	Easy	2	2,2	12 to 16 hours	2	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,3
5	Information Classification and Handling	Principle: An information classification scheme should be established (supported by information handling guidelines) that applies throughout the organisation, based on the confidentiality of information. Objective: To ensure that information is protected in line with its assigned level of classification.	Easy	2	Easy	2	Neither	3	Very easy	1	Neither	3	Easy	2	2,2	12 to 16 hours	2	1 to 4 hours	5	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
6	Technical Vulnerability Management	Principle: A process should be established for the identification and remediation of technical vulnerabilities in business applications, systems, equipment and devices. Objective: To address technical vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in serious security incidents.	Easy	2	Easy	2	Neither	3	Easy	2	Neither	3	Very easy	1	2,2	12 to 16 hours	2	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
7	Malware Protection Software	Principle: Systems throughout the organisation should be safeguarded against all forms of malware by maintaining up-to-date malware protection software, which is supported by effective procedures for managing malware-related security incidents. Objective: To protect the organisation against malware attacks and ensure malware infections can be addressed within defined timescales.	Easy	2	Neither	3	Neither	3	Easy	2	Easy	2	Very easy	1	2,2	12 to 16 hours	2	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	12 to 16 hours	2	3,7
8	System Build	Principle: System build activities (including program coding and software package customisation) should be carried out in accordance with industry good practice, performed by individuals provided with adequate skills/tools, and inspected to identify unauthorised modifications or changes. Objective: To ensure that systems are built correctly, able to withstand malicious attacks, and help ensure that no security weaknesses are introduced during the build process.	Very easy	1	Easy	2	Difficult	4	Easy	2	Neither	3	Easy	2	2,3	12 to 16 hours	2	12 to 16 hours	2	12 to 16 hours	2	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,7
9	Security Event Logging	Principle: Important security-related events should be recorded in logs, stored centrally, protected against unauthorised change and analysed on a regular basis. Objective: To help identify threats that may lead to an information security incident, maintain the integrity of important security-related information and support forensic investigations.	Difficult	4	Neither	3	Easy	2	Easy	2	Easy	2	Very easy	1	2,3	12 to 16 hours	2	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,3

			Automatability?													Manual time?												
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
10	System Testing	Principle: Systems under development (including application software packages, system software, hardware, communications and services) should be tested in a dedicated testing area that simulates the live environment, before the system is promoted to the live environment. Objective: To ensure systems function as intended, meet predefined security requirements and do not compromise information security.	Easy	2	Easy	2	Neither	3	Easy	2	Neither	3	Easy	2	2,3	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
11	Quality Assurance	Principle: Quality assurance of key security activities should be performed at each stage of the system development lifecycle. Objective: To provide assurance that security requirements are defined adequately, agreed security controls are developed, and security requirements are met.	Easy	2	Easy	2	Neither	3	Neither	3	Neither	3	Easy	2	2,5	12 to 16 hours	2	12 to 16 hours	2	12 to 16 hours	2	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,7
12	Security Testing	Principle: Systems under development should be subject to security testing, using a range of attack types (including vulnerability assessments, penetration testing and access control testing). Objective: To identify security weaknesses in systems and determine how systems will behave under attack conditions.	Neither	3	Neither	3	Easy	2	Easy	2	Neither	3	Easy	2	2,5	12 to 16 hours	2	16 hours or more	1	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	16 hours or more	1	2,7
13	System Promotion Criteria	Principle: Rigorous criteria (including security requirements) should be met before new systems are promoted into the live environment. Objective: To ensure that only security tested and approved versions of system are promoted into the live environment.	Easy	2	Neither	3	Easy	2	Neither	3	Neither	3	Easy	2	2,5	8 to 12 hours	3	12 to 16 hours	2	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,2
14	Browser-based Application Protection	Principle: Specialised procedural and technical controls should be applied to browser-based applications and the servers on which they run. Objective: To ensure that the increased risks associated with browser-based applications are minimised.	Easy	2	Neither	3	Neither	3	Easy	2	Neither	3	Easy	2	2,5	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
15	Business Impact Assessment - Confidentiality Requirements	Principle The business impact of unauthorised disclosure of sensitive business information associated with target environments should be assessed. Objective To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) for information associated with target environments (e.g. critical business environments, processes, applications (including those under development) and supporting systems/networks).	Easy	2	Neither	3	Easy	2	Neither	3	Neither	3	Easy	2	2,5	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
16	Business Impact Assessment - Integrity Requirements	Principle The business impact of the accidental corruption or deliberate manipulation of critical business information associated with target environments should be assessed. Objective To document and agree the integrity requirements (the need for information to be valid, accurate and complete) for information associated with target environments (e.g. critical business environments, processes, applications (including those under development) and supporting systems/networks).	Easy	2	Neither	3	Easy	2	Neither	3	Neither	3	Easy	2	2,5	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
17	Business Impact Assessment - Availability Requirements	Principle The business impact of critical business information associated with target environments being unavailable for any length of time should be assessed. Objective To document and agree the availability requirements (the need for information to be accessible when required) for information associated with target environments (e.g. critical business environments, processes, applications (including those under development) and supporting systems/networks).	Easy	2	Neither	3	Easy	2	Neither	3	Neither	3	Easy	2	2,5	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
18	Access Control Mechanisms - Token	Principle: Target environments (e.g. business applications, systems or network devices) that are configured with access control mechanisms based on tokens, should require users to provide a valid token (e.g. physical token, soft token or smartcard) and any related authentication information before they can gain access to these environments. Objective: To prevent unauthorised users from gaining access to token-protected critical or sensitive information, business applications, information systems, networks or computing devices.	Difficult	4	Easy	2	Easy	2	Easy	2	Neither	3	Easy	2	2,5	8 to 12 hours	3	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	4,5
19	Information Security Projects	Principle: Information security projects (and security-related initiatives) should align with the organisation's project management process, take into account security requirements and be run in a systematic and structured manner. Objective: To ensure that all information security projects apply common project management practices, meet security requirements and are aligned with the organisation's business objectives.	Neither	3	Very difficult	5	Easy	2	Very easy	1	Neither	3	Easy	2	2,7	8 to 12 hours	3	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,0
20	Post-implementation Review	Principle: Post-implementation reviews (including coverage of information security), should be conducted for all new systems. Objective: To provide assurance that information security was considered and addressed throughout each stage of the system development lifecycle (SDLC) and built-in security controls are working as expected.	Easy	2	Neither	3	Easy	2	Easy	2	Very difficult	5	Easy	2	2,7	4 to 8 hours	4	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,5

			Automatability?														Manual time?													
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
21	Intrusion Detection	Principle: Intrusion detection mechanisms should be applied to critical systems and networks. Objective: To identify suspected or actual malicious attacks and enable the organisation to respond before serious damage is done.	Difficult	4	Neither	3	Neither	3	Easy	2	Neither	3	Very easy	1	2,7	12 to 16 hours	2	4 to 8 hours	4	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	3,5
22	Performance Monitoring	Principle: The performance of business applications, systems and networks should be monitored continuously, and reviewed by business owners. Objective: To reduce the likelihood of degraded system performance or unavailability having a negative impact on business operations.	Difficult	4	Easy	2	Neither	3	Easy	2	Neither	3	Easy	2	2,7	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7
23	System Design	Principle: Information security requirements for systems under development should be considered when designing systems. Objective: To produce live systems based on sound design principles which have security functionality built-in, enable controls to be incorporated easily, are able to withstand malicious attacks, and help ensure that no security weaknesses are introduced during the build process.	Neither	3	Difficult	4	Easy	2	Neither	3	Easy	2	Easy	2	2,7	8 to 12 hours	3	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
24	Access Control Mechanisms	Principle: Access to business applications, systems, networks and computing devices should be restricted to authorised individuals by the use of access control mechanisms. Objective: To limit access to only authorised individuals.	Easy	2	Easy	2	Easy	2	Neither	3	Difficult	4	Neither	3	2,7	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
25	Virtual Servers	Principle: Virtual servers should be subject to approval, deployed on robust, secure physical servers and configured to segregate sensitive information. Objective: To prevent business disruption as a result of system overload or disclosure of sensitive information to unauthorised individuals.	Easy	2	Easy	2	Easy	2	Easy	2	Very difficult	5	Neither	3	2,7	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
26	Business Impact Assessment	Principle: The potential realistic and worst-case business impact (should critical or sensitive information in the target environment be compromised) should be determined for different categories of impact (e.g. financial, operational, legal and regulatory compliance, reputational and health and safety). Objective: To determine the business impact that business owners are willing to accept in the event information in the target environments is compromised; and agree the requirements for protecting the confidentiality, integrity and availability of that information.	Easy	2	Difficult	4	Neither	3	Easy	2	Neither	3	Easy	2	2,7	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
27	Information Risk Assessment - Supporting Material	Principle: Important material required to support each stage of information risk assessments should be developed, approved and made available throughout the organisation. Objective: To ensure that each phase of risk assessments are performed correctly, provide practical results and enable effective decisions about risk to be made.	Difficult	4	Neither	3	Easy	2	Easy	2	Difficult	4	Easy	2	2,8	8 to 12 hours	3	16 hours or more	1	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	2,8
28	Access Control	Principle: Access control arrangements should be established to restrict access to business applications, systems, networks and computing devices by all types of user, who should be assigned specific privileges to restrict them to particular information or systems. Objective: To ensure that only authorised individuals gain access to business applications, information systems, networks and computing devices, that individual accountability is assured and to provide authorised users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.	Easy	2	Easy	2	Difficult	4	Neither	3	Neither	3	Neither	3	2,8	16 hours or more	1	4 to 8 hours	4	16 hours or more	1	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	2,8
29	Network Device Configuration	Principle: Network devices should be configured to function as required, and to prevent unauthorised or incorrect updates. Objective: To ensure that the configuration of network devices is accurate and does not compromise the security of the network.	Difficult	4	Easy	2	Easy	2	Easy	2	Difficult	4	Neither	3	2,8	16 hours or more	1	8 to 12 hours	3	8 to 12 hours	3	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,8
30	Vulnerability Assessment	Principle: A process should be established to identify and assess the vulnerabilities and related controls in the target environment. Objective: To evaluate the degree to which the assets in scope are vulnerable to threat events.	Difficult	4	Easy	2	Neither	3	Easy	2	Difficult	4	Easy	2	2,8	8 to 12 hours	3	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,0
31	System Development Methodology	Principle: Development activities should be conducted in accordance with a documented system development methodology. Objective: To ensure that systems (including those under development) meet business and information security requirements.	Easy	2	Neither	3	Very difficult	5	Easy	2	Neither	3	Easy	2	2,8	12 to 16 hours	2	12 to 16 hours	2	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,2
32	Email	Principle: Email systems should be protected by a combination of policy, awareness, procedural and technical security controls. Objective: To ensure that email services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.	Easy	2	Easy	2	Difficult	4	Very difficult	5	Neither	3	Very easy	1	2,8	4 to 8 hours	4	8 to 12 hours	3	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,3

			Automatability?														Manual time?													
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
33	Mobile Device Connectivity	Principle: Mobile devices (including laptops, tablets and smartphones) should be provided with secure means of connecting to other devices and to networks. Objective: To ensure mobile devices are protected against unauthorised access and to prevent the unauthorised disclosure of information.	Neither	3	Easy	2	Easy	2	Very difficult	5	Neither	3	Easy	2	2,8	12 to 16 hours	2	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,5
34	Specifications of Requirements	Principle: System requirements (including those for information security) should be documented in the business requirements and agreed before detailed design commences. Objective: To ensure that information security requirements are treated as an integral part of business requirements, fully considered and approved.	Neither	3	Very difficult	5	Neither	3	Easy	2	Easy	2	Easy	2	2,8	4 to 8 hours	4	16 hours or more	1	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
35	Network Storage Systems	Principle: Network storage systems should be protected using system and network controls. Objective: To ensure network storage systems operate as intended, are available when required and do not compromise the security of information they store.	Easy	2	Easy	2	Easy	2	Neither	3	Very difficult	5	Neither	3	2,8	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
36	Emergency Fixes	Principle: Emergency fixes to business information, business applications and technical infrastructure should be tested, reviewed and applied quickly and effectively, in accordance with documented standards/procedures. Objective: To respond to emergencies in a timely and secure manner, while reducing disruption to the organisation.	Easy	2	Easy	2	Easy	2	Easy	2	Difficult	4	Very difficult	5	2,8	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
37	User Authorisation	Principle: Individuals with access to business applications, systems, networks and computing devices should be authorised before they are granted access privileges. Objective: To restrict access to business applications, information, networks and computing devices to authorised users.	Neither	3	Easy	2	Easy	2	Difficult	4	Neither	3	Neither	3	2,8	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
38	Identity and Access Management	Principle: Identity and access management arrangements should be established to provide effective and consistent user administration, identification, authentication and access control mechanisms across the organisation. Objective: To restrict system access to authorised users and ensure the integrity of important information.	Easy	2	Neither	3	Neither	3	Neither	3	Neither	3	Difficult	4	3,0	8 to 12 hours	3	8 to 12 hours	3	16 hours or more	1	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,0
39	Mobile Device Protection	Principle: Mobile devices (including laptops, tablets and smartphones) should be built using standard technical configurations and subject to security management practices to protect information against loss, theft and unauthorised disclosure. Objective: To ensure mobile devices do not compromise the security of information stored on them or processed by them, and prevent unauthorised access to information in the event they are lost or stolen.	Very difficult	5	Easy	2	Easy	2	Very difficult	5	Easy	2	Easy	2	3,0	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,3
40	System Development Environments	Principle: System development activities should be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access. Objective: To provide a secure environment for system development activities, and avoid any disruption to business activity.	Difficult	4	Neither	3	Difficult	4	Easy	2	Neither	3	Easy	2	3,0	8 to 12 hours	3	4 to 8 hours	4	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,3
41	Server Configuration	Principle: Servers should be configured to function as required, and to prevent unauthorised or incorrect updates. Objective: To ensure servers operate as intended and do not compromise the security of computer installations or other environments.	Difficult	4	Easy	2	Difficult	4	Easy	2	Neither	3	Neither	3	3,0	16 hours or more	1	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,3
42	Enterprise Mobility Management	Principle: Smartphones, tablets and other devices using mobile operating systems (e.g. iOS and Android), and the applications ('apps') that run on them, should be protected in the event of loss, theft or cyber attack by deploying an Enterprise Mobility Management (EMM) system. Objective: To ensure that critical and sensitive information handled by individuals working with smartphones and tablets is adequately protected.	Difficult	4	Easy	2	Easy	2	Very difficult	5	Neither	3	Easy	2	3,0	12 to 16 hours	2	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,5
43	Ownership and Responsibilities	Principle: Ownership of critical business environments, processes, applications (including supporting technical infrastructure) and information should be assigned to capable individuals, supported by responsibilities for protecting them that are clearly defined and accepted. Objective: To achieve individual accountability for information and systems, provide a sound management structure for individuals running or using them and give their owners a vested interest in their protection.	Easy	2	Easy	2	Neither	3	Easy	2	Very difficult	5	Difficult	4	3,0	12 to 16 hours	2	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7

			Automatability?														Manual time?													
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
44	Remote Working	Principle: Individuals working in remote environments (e.g. in locations other than the organisation's premises) should: be subject to authorisation; protect computing devices and the information they handle against loss, theft and cyber attack; be supported by security awareness material; and employ additional security controls when travelling to high risk countries or regions. Objective: To ensure that critical and sensitive information handled by individuals working in remote environments is protected against the full range of threats to that information.	Easy	2	Easy	2	Neither	3	Very difficult	5	Neither	3	Neither	3	3,0	12 to 16 hours	2	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	8 to 12 hours	3	3,7
45	Sign-on Process	Principle: Users should be subject to a rigorous sign-on process before being provided with access to business applications, systems, networks and computing devices. Objective: To ensure that only authorised users can gain access to business applications, information systems, networks and computing devices.	Difficult	4	Neither	3	Easy	2	Easy	2	Difficult	4	Neither	3	3,0	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,7
46	Voice Communication Services	Principle: Voice communication services should be approved, protected by a combination of general network and technology-specific controls, monitored regularly and supported by access restrictions. Objective: To ensure the availability of voice communication services, and protect the confidentiality and integrity of sensitive information (e.g. the content of calls) in transit.	Easy	2	Neither	3	Neither	3	Very difficult	5	Neither	3	Easy	2	3,0	4 to 8 hours	4	4 to 8 hours	4	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7
47	Wireless Access	Principle: Wireless access should be subject to authorisation, authentication of users and computing devices, and encryption of wireless traffic. Objective: To ensure that only authorised individuals and computing devices gain wireless access to networks and minimise the risk of wireless transmissions being monitored, intercepted or modified.	Easy	2	Easy	2	Easy	2	Very difficult	5	Very difficult	5	Easy	2	3,0	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
48	Malware Protection Activities	Principle: Activities should be performed to make users aware of the risks from malware, and to specify the actions required to minimise those risks. Objective: To ensure all relevant individuals understand the key elements of malware protection, why it is needed, and help to keep the impact of malware to a minimum.	Difficult	4	Easy	2	Easy	2	Very difficult	5	Difficult	4	Very easy	1	3,0	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	12 to 16 hours	2	4,0
49	Risk Evaluation	Principle: Information risk should be evaluated based on analysis of threats, vulnerabilities, controls and business impact. Objective: To determine the risk to assets in the target environment.	Difficult	4	Easy	2	Neither	3	Difficult	4	Difficult	4	Easy	2	3,2	8 to 12 hours	3	16 hours or more	1	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,0
50	Portable Storage Devices	Principle: The use of portable storage devices (e.g. USB memory sticks, external hard disk drives, media players and e-book readers) should be subject to approval, access to them restricted, and information stored on them protected. Objective: To ensure that sensitive information stored on portable storage devices is protected from unauthorised disclosure.	Very difficult	5	Easy	2	Easy	2	Very difficult	5	Neither	3	Easy	2	3,2	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,3
51	Information Validation	Principle: Business applications should incorporate security controls that protect the confidentiality and integrity of information when it is input into, processed by and output from these applications. Objective: To protect the integrity (validity, accuracy, completeness and timeliness) of critical information, stored in or processed by business applications.	Neither	3	Difficult	4	Neither	3	Difficult	4	Neither	3	Easy	2	3,2	4 to 8 hours	4	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,5
52	Customer Connections	Principle: Access to business applications by customers should be uniquely identified, recorded in an inventory of connections, protected using access control mechanisms and monitored. Objective: To protect the confidentiality, integrity and availability of critical or sensitive information relating to either the organisation or the customer.	Very difficult	5	Difficult	4	Easy	2	Easy	2	Neither	3	Neither	3	3,2	4 to 8 hours	4	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,5
53	Collaboration Platforms	Principle: Collaboration platforms should be protected by setting management policy, deploying application controls, configuring the security settings of each platform and improving the security of supporting technical infrastructure. Objective: To ensure that collaboration platforms are available when required, the confidentiality and integrity of information is protected in transit, and the risk of misuse is minimised.	Difficult	4	Easy	2	Neither	3	Very difficult	5	Neither	3	Easy	2	3,2	8 to 12 hours	3	4 to 8 hours	4	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
54	Customer Contracts	Principle: All customer access to the organisation's business applications should be supported by agreed, approved contracts, which cover security arrangements. Objective: To ensure customers are legally and contractually bound to protect the organisation's information, business applications and systems, and the organisation's security obligations are met.	Difficult	4	Neither	3	Easy	2	Very difficult	5	Easy	2	Neither	3	3,2	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7

			Automatability?														Manual time?													
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
55	Cryptographic Key Management	Principle: Cryptographic keys should be managed tightly, in accordance with documented standards/procedures, and protected against unauthorised access or destruction. Objective: To ensure that cryptographic keys are not compromised (e.g. through loss, corruption or disclosure), thereby exposing critical or sensitive information to attack.	Easy	2	Difficult	4	Easy	2	Very difficult	5	Difficult	4	Easy	2	3,2	12 to 16 hours	2	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	8 to 12 hours	3	3,7
56	Access Control Mechanisms - Biometric	Principle: Target environments (e.g. business applications, systems or networks and computing devices) that are configured with access control mechanisms based on biometrics, should require users to provide a valid biometric (e.g. fingerprint/vein recognition, iris/retina patterns or voice characteristics) and any related authentication information before they can gain access to these environments. Objective: To prevent unauthorised users from gaining access to biometric-protected critical or sensitive information, business applications, information systems, networks or computing devices.	Difficult	4	Easy	2	Easy	2	Easy	2	Difficult	4	Very difficult	5	3,2	8 to 12 hours	3	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
57	Security Awareness Programme	Principle: Specific activities should be undertaken, such as a security awareness programme, to promote and embed expected security behaviour in all individuals who have access to the organisation's information and systems. Objective: To create a culture where expected security behaviour is embedded and where all relevant individuals make effective risk-based decisions and protect critical and sensitive information used throughout the organisation from being compromised.	Very easy	1	Easy	2	Neither	3	Very difficult	5	Very difficult	5	Neither	3	3,2	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,2
58	Legal and Regulatory Compliance	Principle: A process should be established to identify and interpret the information security implications of relevant laws and regulations. Objective: To comply with laws and regulations affecting information security.	Easy	2	Difficult	4	Neither	3	Neither	3	Very difficult	5	Neither	3	3,3	16 hours or more	1	8 to 12 hours	3	4 to 8 hours	4	16 hours or more	1	4 to 8 hours	4	16 hours or more	1	2,3
59	Document Management	Principle: Documents should be managed in a systematic, structured manner, and information security requirements met throughout the document lifecycle. Objective: To protect information contained in documents in accordance with legal requirements, ensure critical information remains available when required, preserve the integrity of critical information and protect sensitive information from unauthorised disclosure.	Easy	2	Difficult	4	Neither	3	Very difficult	5	Difficult	4	Easy	2	3,3	16 hours or more	1	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,7
60	Threat Profiling	Principle: Threats and related threat events to target environments should be identified, profiled, prioritised and recorded. Objective: To identify threats, prioritise them (e.g. based on threat strength), determine related threat events and assess the likelihood of threat events occurring in the target environment (i.e. likelihood of initiation).	Difficult	4	Difficult	4	Neither	3	Neither	3	Difficult	4	Easy	2	3,3	16 hours or more	1	4 to 8 hours	4	8 to 12 hours	3	8 to 12 hours	3	1 to 4 hours	5	16 hours or more	1	2,8
61	Information Risk Assessment - Methodology	Principle: Information risk assessments should be undertaken using systematic and structured methodologies. Objective: To make information risk assessments effective, easy to conduct and consistent throughout the organisation and to produce a clear picture of key information risks.	Neither	3	Difficult	4	Easy	2	Neither	3	Difficult	4	Difficult	4	3,3	4 to 8 hours	4	1 to 4 hours	5	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
62	Remote Maintenance	Principle: Remote maintenance of critical systems and networks should be restricted to authorised individuals, confined to individual sessions, and subject to review. Objective: To prevent unauthorised access to critical systems and networks through the misuse of remote maintenance facilities.	Difficult	4	Easy	2	Neither	3	Very difficult	5	Neither	3	Neither	3	3,3	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
63	Security Architecture	Principle A security architecture should be established to help manage the complexity of providing information security at scale throughout the organisation. Objective To enable system developers and administrators to make more effective decisions and implement consistent, simple-to-use security functionality across multiple business applications and systems throughout the organisation.	Difficult	4	Very easy	1	Very difficult	5	Easy	2	Very difficult	5	Neither	3	3,3	8 to 12 hours	3	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
64	EUDA Inventory	Principle: Critical End User Developed Applications (EUDA) (e.g. those developed using spreadsheet and database programs) should be recorded in an inventory, or equivalent. Objective: To maintain an accurate and up-to-date record of critical End User Developed Applications (EUDA), enabling them to be protected accordingly.	Difficult	4	Easy	2	Very easy	1	Very difficult	5	Very difficult	5	Neither	3	3,3	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	8 to 12 hours	3	16 hours or more	1	4,0
65	Cloud Service Contracts	Principle: The organisation's use of cloud services should be supported by contracts that include cloud specific clauses beyond standard contracts with external suppliers. Objective: To ensure cloud specific risks are reduced to a level acceptable by the organisation.	Easy	2	Easy	2	Easy	2	Very difficult	5	Very difficult	5	Difficult	4	3,3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	4,0

			Automatability?														Manual time?											
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
66	Information Privacy	Principle: Responsibility for managing information privacy should be established and information security controls applied for handling personally identifiable information (i.e. information that can be used to identify an individual person). Objective: To prevent information about individuals being used in an inappropriate manner, and ensure compliance with legal and regulatory requirements for information privacy.	Difficult	4	Difficult	4	Neither	3	Neither	3	Difficult	4	Neither	3	3,5	12 to 16 hours	2	16 hours or more	1	8 to 12 hours	3	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,7
67	Software Acquisition	Principle: Robust, reliable software should be acquired (e.g. purchased or leased) following consideration of security requirements and identification of any security deficiencies. Objective: To ensure that software acquired from external suppliers provides the required functionality and does not compromise the security of critical or sensitive information and systems.	Difficult	4	Difficult	4	Easy	2	Very difficult	5	Difficult	4	Easy	2	3,5	12 to 16 hours	2	12 to 16 hours	2	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,2
68	Information Risk Assessment - Management Approach	Principle: Information risk assessments should be performed for target environments (e.g. critical business environments, processes and applications (including those under development); and supporting technical infrastructure) on a regular basis. Objective: To enable individuals who are responsible for target environments to identify key information risks, evaluate them and determine the treatment required to keep those risks within acceptable limits.	Neither	3	Difficult	4	Easy	2	Difficult	4	Difficult	4	Difficult	4	3,5	4 to 8 hours	4	8 to 12 hours	3	4 to 8 hours	4	8 to 12 hours	3	1 to 4 hours	5	16 hours or more	1	3,3
69	Firewalls	Principle: Network traffic should be routed through a well-configured firewall prior to being allowed access to networks, or before leaving networks. Objective: To prevent unauthorised network traffic from gaining access to networks, or leaving networks.	Neither	3	Neither	3	Easy	2	Very difficult	5	Very difficult	5	Neither	3	3,5	12 to 16 hours	2	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,3
70	Security Event Management	Principle: Security-related event logs should be reviewed and analysed on a regular basis, by security specialists, using a combination of automated and manual methods. Objective: To identify known vulnerabilities, unusual or suspicious activity, and respond to events that need investigating in a timely manner.	Easy	2	Difficult	4	Neither	3	Difficult	4	Very difficult	5	Neither	3	3,5	8 to 12 hours	3	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
71	Employment Lifecycle	Principle: Information security requirements should be embedded into each stage of the employment lifecycle, specifying security related actions required during the induction of each individual, their ongoing management and termination of their employment. Objective: To ensure that employees are equipped with the skills, knowledge and tools to support the organisation's values and adhere to information security policies.	Difficult	4	Neither	3	Easy	2	Very difficult	5	Neither	3	Difficult	4	3,5	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	12 to 16 hours	2	3,7
72	System Decommission	Principle: Systems that are no longer required should be evaluated and subject to a decommissioning process (where required), taking account of relevant information, software, services, equipment and devices. Objective: To keep information risk associated with systems that are no longer required within acceptable limits.	Easy	2	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	Easy	2	3,5	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,7
73	Business Application Protection	Principle: Business applications should be protected by using sound security architecture principles. Objective: To ensure business applications use consistent security functionality, align with the organisation's technical security infrastructure and protect the information they process.	Difficult	4	Difficult	4	Very difficult	5	Neither	3	Neither	3	Easy	2	3,5	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,7
74	Customer Access Arrangements	Principle: Access to business applications by customers should be established according to business requirements, subject to an information risk assessment and approved by application owners. Objective: To ensure that all aspects of customer access to the organisation's business applications meet security requirements.	Difficult	4	Difficult	4	Very difficult	5	Easy	2	Neither	3	Neither	3	3,5	1 to 4 hours	5	12 to 16 hours	2	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7
75	Security Awareness Messages	Principle: Individuals who have access to the information and systems of the organisation should have tailored and appropriate security messages communicated to them on a regular basis. Objective: To ensure individuals remain aware of the importance and need for information security on an ongoing basis, and maintain a security-positive culture throughout the organisation.	Difficult	4	Easy	2	Neither	3	Very difficult	5	Difficult	4	Neither	3	3,5	1 to 4 hours	5	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8
76	Backup	Principle: Backups of essential information and software should be performed on a regular basis, according to a defined cycle. Objective: To ensure that, in the event of an emergency, essential information or software can be restored within critical timescales.	Difficult	4	Easy	2	Easy	2	Very difficult	5	Neither	3	Very difficult	5	3,5	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,8

			Automatability?														Manual time?											
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
77	Cloud Computing Policy	Principle: A comprehensive, documented policy on the use of cloud services should be produced and communicated to all individuals who may purchase or use cloud services. Objective: To ensure all relevant individuals throughout the organisation are aware of executive management's direction on and requirements regarding the acquisition and use of cloud services.	Difficult	4	Very difficult	5	Easy	2	Difficult	4	Very difficult	5	Very easy	1	3,5	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,8
78	Security Audit Process - Reporting	Principle: The results of security audits of target environments, including findings and recommendations, should be documented and reported to stakeholders. Objective: To ensure stakeholders are informed about the risks associated with target environments and enable owners for remedial actions to be identified and agreed.	Easy	2	Easy	2	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	3,5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,3
79	Risk Treatment	Principle: Risk treatment options for each individual risk should be identified, reviewed and agreed; and associated risk treatment plans approved by executive management. Objective: To ensure information risks are treated in a suitable manner (e.g. mitigated, avoided, transferred or accepted), in line with risk appetite.	Very difficult	5	Difficult	4	Neither	3	Very difficult	5	Neither	3	Easy	2	3,7	8 to 12 hours	3	16 hours or more	1	8 to 12 hours	3	12 to 16 hours	2	4 to 8 hours	4	16 hours or more	1	2,3
80	Computer and Network Installations	Principle: Computer system, network and telecommunication installations (e.g. data centres) should be designed to cope with current and predicted information processing requirements, and be protected using a range of in-built security controls. Objective: To ensure computer system, network and telecommunication installations can meet the security requirements of the critical business applications they support (i.e. protect them against the compromise of confidentiality, integrity and availability of information they process).	Very difficult	5	Neither	3	Neither	3	Neither	3	Very difficult	5	Neither	3	3,7	12 to 16 hours	2	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,3
81	Employee-owned Devices	Principle: Where an organisation allows the use of employee-owned devices for business purposes (including smartphones, tablets and laptops), this should be supported by documented agreements with employees and technical security controls to protect business information. Objective: To ensure that critical and sensitive business information handled on employee-owned devices receives the same level of protection as that typically provided for corporate-owned devices.	Very difficult	5	Neither	3	Easy	2	Very difficult	5	Neither	3	Difficult	4	3,7	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,7
82	Security Audit Process - Monitoring	Principle: Actions to address security audit findings should be incorporated into a programme of work and monitored continuously. Objective: To ensure the risks identified during security audits are treated effectively, compliance requirements are being met, and agreed security controls are being implemented within agreed timescales.	Easy	2	Easy	2	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	3,7	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,2
83	External Network Connections	Principle: All external network connections to systems and networks should be individually identified, verified, recorded, and approved by the system or network owner. Objective: To prevent unauthorised external users from gaining access to information systems and networks.	Difficult	4	Neither	3	Neither	3	Very difficult	5	Very difficult	5	Neither	3	3,8	16 hours or more	1	16 hours or more	1	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	2,7
84	Protection of Databases	Principle: Critical End User Developed Applications (EUDA) created using database programs should be protected by validating input, implementing access control, and restricting user access to powerful functionality. Objective: To assure the accuracy of information processed by critical databases, and protect that information from disclosure to unauthorised individuals.	Difficult	4	Difficult	4	Difficult	4	Very difficult	5	Neither	3	Neither	3	3,8	12 to 16 hours	2	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,8
85	Cryptographic Solutions	Principle: Cryptographic solutions should be subject to approval, documented and applied throughout the organisation. Objective: To protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of transactions or communications.	Difficult	4	Very difficult	5	Neither	3	Neither	3	Difficult	4	Difficult	4	3,8	8 to 12 hours	3	16 hours or more	1	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,0
86	Protection of Spreadsheets	Principle: Critical End User Developed Applications (EUDA) created using spreadsheet programs should be protected by validating input, implementing access control and restricting user access to powerful functionality. Objective: To assure the accuracy of information processed by critical spreadsheets, and protect that information from disclosure to unauthorised individuals.	Very difficult	5	Difficult	4	Difficult	4	Very difficult	5	Easy	2	Neither	3	3,8	8 to 12 hours	3	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,3
87	Local Environment Profile	Principle: A security profile for each local environment should be documented and maintained, which contains important business and security details about business users, information, business applications, equipment, technology and locations. Objective: To provide a high-level picture of the type and importance of business conducted in the local environment, which helps support security decisions about activities relating to the local environment.	Difficult	4	Easy	2	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	3,8	16 hours or more	1	1 to 4 hours	5	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,3

			Automatability?														Manual time?											
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
88	Information Security Policy	Principle: A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the organisation's information and systems. Objective: To document the governing body's direction on and commitment to information security, and communicate it to all relevant individuals.	Very difficult	5	Very difficult	5	Easy	2	Neither	3	Very difficult	5	Neither	3	3,8	16 hours or more	1	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
89	Threat Intelligence	Principle: A threat intelligence capability should be established, supported by an intelligence cycle and analytical tools. Objective: To provide information and situational awareness about past, present and predicted attacks, supporting information risk-related decisions and actions.	Difficult	4	Neither	3	Neither	3	Neither	3	Very difficult	5	Very difficult	5	3,8	12 to 16 hours	2	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
90	Security Monitoring and Reporting	Principle: Information security performance should be monitored regularly and reported to specific audiences, such as executive management. Objective: To provide each audience with a relevant, accurate, comprehensive and coherent assessment of information security performance.	Difficult	4	Neither	3	Neither	3	Neither	3	Very difficult	5	Very difficult	5	3,8	1 to 4 hours	5	8 to 12 hours	3	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,5
91	Public Key Infrastructure	Principle: Where a Public Key Infrastructure (PKI) is used, one or more Certification Authorities (CAs) and Registration Authorities (RAs) should be established and protected. Objective: To ensure that the PKI operates as intended, is available when required, provides adequate protection of related cryptographic keys and can be recovered in the event of an emergency.	Difficult	4	Neither	3	Neither	3	Very difficult	5	Very difficult	5	Neither	3	3,8	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	12 to 16 hours	2	3,7
92	Security Incident Management Process	Principle: Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process. Objective: To identify and resolve information security incidents quickly and effectively, minimise their business impact and reduce the risk of similar incidents occurring.	Difficult	4	Difficult	4	Easy	2	Neither	3	Very difficult	5	Very difficult	5	3,8	4 to 8 hours	4	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7
93	Acceptable Use Policies	Principle: Acceptable use policies (AUPs) should be established, which define the organisation's rules on how each individual (e.g. an employee or contractor) can use information and systems, including software, computer equipment and connectivity. Objective: To prevent individuals from inadvertently increasing risk to information and systems.	Neither	3	Very difficult	5	Easy	2	Very difficult	5	Very difficult	5	Neither	3	3,8	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
94	Information Security Assurance	Principle: The organisation should implement a consistent and structured information security assurance programme. Objective: To provide assurance that information security is being implemented effectively.	Difficult	4	Very difficult	5	Very difficult	5	Neither	3	Very difficult	5	Easy	2	4,0	8 to 12 hours	3	16 hours or more	1	16 hours or more	1	16 hours or more	1	1 to 4 hours	5	16 hours or more	1	2,0
95	Stakeholder Value Delivery	Principle: The organisation should implement processes to measure the value delivered by information security initiatives and report the results to all stakeholders. Objective: To ensure that the information security programme delivers value to stakeholders.	Difficult	4	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	Easy	2	4,0	16 hours or more	1	16 hours or more	1	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	12 to 16 hours	2	2,7
96	Security Audit Process - Fieldwork	Principle: Security audit fieldwork conducted for target environments should include collecting relevant background material, performing security audit tests and recording the results of the tests. Objective: To identify both non-compliances and information risks associated with target environments.	Neither	3	Neither	3	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	4,0	8 to 12 hours	3	16 hours or more	1	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	2,8
97	Outsourcing	Principle: A process should be established to govern the selection and management of outsource providers (including cloud service providers), supported by documented agreements that specify the security requirements to be met. Objective: To ensure that security requirements are satisfied and maintained when functions or services are delivered by outsourced providers.	Difficult	4	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	Neither	3	4,0	12 to 16 hours	2	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,2
98	Hardware lifecycle Management	Principle: Robust, reliable hardware should only be acquired (e.g. purchased or leased) following consideration of security requirements and identification of security deficiencies. Objective: To ensure that hardware provides the required functionality and does not compromise the security of critical or sensitive information and systems.	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Easy	2	4,0	12 to 16 hours	2	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,3

			Automatability?													Manual time?													
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
99	Security Education/Training	Principle: Individuals should be educated/trained in how to run systems and applications correctly and how to develop and apply information security controls. Objective: To provide individuals with the skills required to protect information and systems and fulfil their information security responsibilities.	Difficult	4	Neither	3	Neither	3	Very difficult	5	Very difficult	5	Difficult	4	4,0	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,5
100	Risk Assessment Scope	Principle: The scope of information risk assessments should be clearly defined, covering business and technical elements of the target environment and relevant external factors, before assessments are started. Objective: To establish clear limits for information risk assessments (including what is out of scope), and ensure that subsequent activities are appropriate for the profile of the target environment.	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	Difficult	4	Easy	2	4,0	12 to 16 hours	2	12 to 16 hours	2	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	3,7
101	Service Level Agreements	Principle: Computer and network services that support critical business processes and applications should only be obtained from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements. Objective: To define the business requirements for providers of any computer or network services, including those for information security, and to ensure they are met.	Easy	2	Difficult	4	Very difficult	5	Very difficult	5	Neither	3	Very difficult	5	4,0	4 to 8 hours	4	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7
102	Information Risk Reporting	Principle: Reports relating to information risk should be produced and presented to executive management on a regular basis. Objective: To provide executive management with an accurate, comprehensive and coherent view of information risk across the organisation.	Difficult	4	Difficult	4	Neither	3	Very difficult	5	Very difficult	5	Neither	3	4,0	1 to 4 hours	5	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
103	Business Continuity Arrangements	Principle: Alternative business continuity arrangements (sometimes referred to as disaster recovery plans) should be established for individual business environments, and made available when required. Objective: To enable critical business processes to be resumed to an agreed level, within an agreed time following a disruption, using alternative processing facilities.	Difficult	4	Easy	2	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	4,0	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,2
104	Digital Rights Management	Principle: High-value sensitive information or software that is accessed and used outside of the control of the organisation should be protected by the use of digital rights management (DRM). Objective: To ensure that the access to and processing of highly sensitive information is restricted to specific functions by a limited number of authorised individuals.	Neither	3	Difficult	4	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	4,2	4 to 8 hours	4	8 to 12 hours	3	8 to 12 hours	3	4 to 8 hours	4	16 hours or more	1	16 hours or more	1	2,7
105	External Supplier Management Process	Principle: Information risks should be identified and managed throughout all stages of the relationship with external suppliers (including organisations in the supply chain). Objective: To protect critical and sensitive information when being handled by external suppliers (including organisations in the supply chain) or when being transmitted between the organisation and external suppliers.	Difficult	4	Difficult	4	Neither	3	Very difficult	5	Very difficult	5	Difficult	4	4,2	12 to 16 hours	2	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,2
106	Forensic Investigations	Principle: A process should be established for dealing with information security incidents or other events (e.g. e-discovery requests) that require forensic investigation. Objective: To identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.	Difficult	4	Difficult	4	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	4,2	8 to 12 hours	3	8 to 12 hours	3	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,2
107	Resilient Technical Environments	Principle: Critical business applications and underlying technical infrastructure should be run on robust, reliable hardware and software, and be supported by alternative or duplicate facilities. Objective: To ensure critical business processes that rely on business applications and technical infrastructure are available when required.	Easy	2	Difficult	4	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	4,2	8 to 12 hours	3	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,3
108	Industrial Control Systems	Principle: Information systems that monitor or control physical activities should be identified, categorised and protected by security arrangements that are tailored to operate in those environments. Objective: To enable an organisation to manage information risks to industrial control systems (ICS).	Easy	2	Difficult	4	Very difficult	5	Very difficult	5	Difficult	4	Very difficult	5	4,2	4 to 8 hours	4	8 to 12 hours	3	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,5
109	Data Leakage Prevention	Principle: Data leakage prevention solutions should be applied to devices, systems and networks that process, store or transmit sensitive information. Objective: To prevent sensitive information from being disclosed to unauthorised individuals or systems.	Difficult	4	Difficult	4	Very difficult	5	Neither	3	Difficult	4	Very difficult	5	4,2	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,8
110	Business Continuity Planning	Principle: Business continuity plans should be developed and documented to support critical business processes throughout the organisation. Objective: To provide relevant individuals with a documented set of actions to perform in the event of a disaster or emergency affecting business applications and technical infrastructure, enabling critical business processes to be resumed within critical timescales.	Very difficult	5	Easy	2	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	4,2	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,2

			Automatability?														Manual time?													
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
111	EUDA Development	Principle: Development of End User Developed Applications (EUDA) should be carried out in accordance with a documented development methodology. Objective: To ensure EUDA function correctly and meet security requirements.	Difficult	4	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	Neither	3	4,3	12 to 16 hours	2	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,8
112	Information Security Compliance Management	Principle: A security compliance management process should be established, which comprises information security controls derived from regulatory and legal drivers and contracts. Objective: To ensure information security controls are consistently prioritised and addressed according to information security obligations associated with legislation, regulations, contracts, industry standards and organisational policies.	Very difficult	5	Difficult	4	Very difficult	5	Neither	3	Very difficult	5	Difficult	4	4,3	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,7
113	Power Supplies	Principle: Critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) should be protected against power outages. Objective: To prevent critical services from being disrupted by loss of power.	Difficult	4	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,3	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,3
114	Cyber Attack Protection	Principle: Arrangements should be made to protect the organisation's information and systems against sophisticated, targeted cyber attacks. Objective: To reduce the frequency and impact of attempted and successful targeted cyber attacks.	Difficult	4	Very difficult	5	Very difficult	5	Neither	3	Very difficult	5	Very difficult	5	4,5	12 to 16 hours	2	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,8
115	Security Incident Management Framework	Principle: An information security incident management framework should be established, including relevant individuals, information and tools required by the organisation's information security incident management process. Objective: To provide the resources required to help resolve information security incidents quickly and effectively.	Easy	2	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,5	12 to 16 hours	2	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,0
116	Office Equipment	Principle: Office equipment (e.g. printers, photocopiers and multifunction devices) should be approved, protected by software controls and located in physically secure locations. Objective: To ensure information stored in or processed by office equipment is not disclosed to unauthorised individuals.	Very difficult	5	Difficult	4	Very difficult	5	Very difficult	5	Neither	3	Very difficult	5	4,5	4 to 8 hours	4	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,2
117	Physical Network Management	Principle: Networks (including voice networks) should be protected by physical controls and supported by accurate, up-to-date documentation and labelling of essential components. Objective: To ensure that networks (including voice networks) are configured accurately and securely and provide employees with a clear statement of the security disciplines they are expected to follow.	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Neither	3	4,5	8 to 12 hours	3	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	16 hours or more	1	3,3
118	Security Audit Process - Planning	Principle: Security audits of target environments should be subject to thorough planning, which includes identifying risks, determining audit objectives, defining the approach and scope of security audits, and preparing a security audit plan. Objective: To ensure security audits are performed using an agreed methodology, can be completed within acceptable timescales and that no audit steps or activities are missed.	Difficult	4	Very difficult	5	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	4,5	4 to 8 hours	4	16 hours or more	1	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,3
119	Local Security Coordination	Principle: Arrangements should be made to coordinate information security activity in individual business units/departments. Objective: To ensure that security activities are carried out in a timely and accurate manner, throughout the organisation, and that security issues are resolved effectively.	Difficult	4	Very difficult	5	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	4,5	1 to 4 hours	5	12 to 16 hours	2	4 to 8 hours	4	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	3,5
120	Business Continuity Testing	Principle: Business continuity plans and arrangements should be tested on a regular basis. Objective: To provide assurance that business continuity plans and arrangements will work as required, so that critical business processes can resume within predefined timescales.	Neither	3	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,5	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,5
121	Hazard Protection	Principle: Critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) should be protected against fire, flood, environmental and other natural hazards. Objective: To prevent services being disrupted by damage to critical facilities caused by fire, flood and other types of hazard.	Difficult	4	Neither	3	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,5	1 to 4 hours	5	4 to 8 hours	4	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	16 hours or more	1	3,8

			Automatability?														Manual time?											
#	2018 Standard Statement	Explanatory Text	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average	R1	#	R2	#	R3	#	R4	#	R5	#	R6	#	Average
122	Information Security Strategy	Principle: An information security strategy should be maintained that is demonstrably integrated with the organisation's strategic objectives. Objective: To ensure that the information security programme and related security projects contribute to the organisation's success.	Difficult	4	Very difficult	5	Very difficult	5	Difficult	4	Very difficult	5	Difficult	4	4,5	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	4 to 8 hours	4	1 to 4 hours	5	4,3
123	Security Direction	Principle: Control over information security should be provided by a high-level working group, committee or equivalent body, and managed by a board-level executive (or equivalent). Objective: To provide a top-down management structure and mechanism for coordinating security activity (e.g. an information security programme) and supporting the information security governance approach.	Difficult	4	Very difficult	5	Very difficult	5	Neither	3	Very difficult	5	Very difficult	5	4,5	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	4,5
124	Business Continuity Programme	Principle: A business continuity programme should be established, which includes developing a resilient technical infrastructure, creating a crisis management capability, and coordinating and maintaining business continuity plans and arrangements across the organisation. Objective: To enable the organisation to withstand the prolonged unavailability of critical information, business applications and related technical infrastructure, and provide individuals with a documented set of actions to perform in the event of a disaster or emergency.	Difficult	4	Very difficult	5	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	4,7	12 to 16 hours	2	4 to 8 hours	4	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,3
125	Security Audit Management	Principle: The information security status of target environments (e.g. critical business environments, processes, applications and supporting technical infrastructure) should be subject to thorough, independent and regular security audits. Objective: To ensure that security controls have been implemented effectively, that risk is being adequately managed and to provide the owners of target environments and executive management with an independent assessment of their security status.	Difficult	4	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,7	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
126	Security Governance Framework	Principle: A framework for information security governance should be established, and commitment demonstrated by the organisation's governing body. Objective: To ensure that the organisation's overall approach to information security supports high standards of governance.	Very difficult	5	Very difficult	5	Very difficult	5	Neither	3	Very difficult	5	Very difficult	5	4,7	16 hours or more	1	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	4,3
127	Business Continuity Strategy	Principle: A business continuity strategy covering the whole organisation should be established, which promotes the need for business continuity management, embeds business continuity management into the organisation's culture, and is implemented in the form of a business continuity programme. Objective: To align business continuity goals with the organisation's business goals, provide resilience against disruption and minimise impact to the organisation in the event of a disaster or emergency.	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,8	8 to 12 hours	3	12 to 16 hours	2	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,2
128	Crisis Management	Principle: A crisis management process should be established, supported by a crisis management team, which details actions to be taken in the event of a major incident or serious attack. Objective: To respond to major incidents and serious attacks quickly and effectively, reducing any potential business impact including brand and reputational damage.	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,8	8 to 12 hours	3	1 to 4 hours	5	8 to 12 hours	3	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	3,7
129	Physical Protection	Principle: All critical facilities (including locations that house critical technical infrastructure, industrial control systems and specialised equipment) should be physically protected against accident or attack and unauthorised physical access. Objective: To restrict physical access to authorised individuals, ensure that critical facilities are available when required and to prevent important services from being disrupted by loss of, or damage to, equipment or services.	Difficult	4	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	4,8	1 to 4 hours	5	4 to 8 hours	4	4 to 8 hours	4	1 to 4 hours	5	1 to 4 hours	5	16 hours or more	1	4,0
130	Sensitive Physical Information	Principle: Sensitive information held in physical form (sensitive physical information) should be identified, documented, classified and protected throughout its lifecycle. Objective: To protect sensitive physical information in accordance with information security and regulatory requirements, preserve the integrity of sensitive physical information and protect it from corruption, loss and unauthorised disclosure.	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	5,0	1 to 4 hours	5	16 hours or more	1	16 hours or more	1	1 to 4 hours	5	4 to 8 hours	4	16 hours or more	1	2,8
131	Information Security Function	Principle: A specialist information security function should be established, which has responsibility for promoting information security throughout the organisation. Objective: To ensure good practice in information security is applied effectively and consistently throughout the organisation.	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	Very difficult	5	5,0	12 to 16 hours	2	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	1 to 4 hours	5	4,5

Bijlage 5 - Transcripten interviews

Als aparte en vertrouwelijke bijlage opgenomen, kan opgevraagd worden bij de Open Universiteit.

Naam document: Bijlage 5 - Transcripten interviews

Bijlage 6 - Framework voor Continuous Compliance

Zie volgende pagina

Open University of the Netherlands, faculty of Management, Science & Technology
Master Business Process Management & IT
Thesis: Implementation of Continuous Compliance
Author: Nese Ozkanli
Year: 2020

Framework Reference Card for Continuous Compliance
Automation of Information Security Measures in Deployment Pipelines

Easy to automate (39)

- Access Control Mechanisms - Password
- Business Application Register
- Installation Process
- Change Management
- Information Classification and Handling
- Technical Vulnerability Management
- Malware Protection Software
- System Build
- Security Event Logging
- System Testing
- Quality Assurance
- Security Testing
- System Promotion Criteria
- Browser-based Application Protection
- Business Impact Assessment - Confidentiality Requirements
- Business Impact Assessment - Integrity Requirements
- Business Impact Assessment - Availability Requirements
- Access Control Mechanisms - Token
- Information Security Projects
- Post-implementation Review
- Performance Monitoring
- System Design
- Access Control Mechanisms
- Virtual Servers
- Business Impact Assessment
- Information Risk Assessment - Supporting Material
- Network Device Configuration
- Vulnerability Assessment
- System Development Methodology
- Email
- Mobile Device Connectivity
- Specifications of Requirements
- Network Storage Systems
- Emergency Fixes
- Mobile Device Protection
- Enterprise Mobility Management
- Ownership and Responsibilities
- Wireless Access
- Portable Storage Devices

Difficult to automate (69)

- Risk Evaluation
- Security Awareness Programme
- Document Management
- Threat Profiling
- Information Risk Assessment - Methodology
- Security Architecture
- EUDA Inventory
- Information Privacy
- Software Acquisition
- Information Risk Assessment - Management Approach
- Security Event Management
- Employment Lifecycle
- Business Application Protection
- Customer Access Arrangements
- Security Awareness Messages
- Backup
- Cloud Computing Policy
- Risk Treatment
- Employee-owned Devices
- Security Audit Process - Monitoring
- External Network Connections
- Protection of Databases
- Cryptographic Solutions
- Protection of Spreadsheets
- Local Environment Profile
- Information Security Policy
- Threat Intelligence
- Security Monitoring and Reporting
- Public Key Infrastructure
- Security Incident Management Process
- Acceptable Use Policies
- Information Security Assurance
- Stakeholder Value Delivery
- Security Audit Process - Fieldwork
- Outsourcing
- Hardware lifecycle Management
- Security Education/Training
- Risk Assessment Scope
- Service Level Agreements
- Information Risk Reporting
- Business Continuity Arrangements
- Digital Rights Management
- External Supplier Management Process
- Forensic Investigations
- Resilient Technical Environments
- Industrial Control Systems
- Data Leakage Prevention
- Business Continuity Planning
- EUDA Development
- Information Security Compliance Management
- Power Supplies
- Cyber Attack Protection
- Security Incident Management Framework
- Office Equipment
- Physical Network Management
- Security Audit Process - Planning
- Local Security Coordination
- Business Continuity Testing
- Hazard Protection
- Information Security Strategy
- Security Direction
- Business Continuity Programme
- Security Audit Management
- Security Governance Framework
- Business Continuity Strategy
- Crisis Management
- Physical Protection
- Sensitive Physical Information
- Information Security Function

Needs more investigation (23)

- Intrusion Detection
- Access Control
- User Authorisation
- Identity and Access Management
- Computer and Network Installations
- System Development Environments
- Server Configuration
- Remote Working
- Sign-on Process
- Voice Communication Services
- Malware Protection Activities
- Information Validation
- Customer Connections
- Collaboration Platforms
- Customer Contracts
- Cryptographic Key Management
- Access Control Mechanisms - Biometric
- Legal and Regulatory Compliance
- Remote Maintenance
- Cloud Service Contracts
- Firewalls
- System Decommission
- Security Audit Process – Reporting

Based on ISF Standard of Good Practice for Information Security (2018)